

# INTERNSHIP PROJECT NO. 2

**Supritijui2000@gmail.com**

## System Hacking: -

## 1. Check for SMTP open relay

An open relay is a Simple Mail Transfer Protocol (SMTP) email server that allows anyone on the Internet to send messages through it while hiding or obscuring the source of the messages being sent. Open relays do nothing to identify the original sender of email messages, making them very vulnerable to address spoofing, a technique that alters email headers to appear as though they originated from a source other than the actual source. Although this is how email was initially set up, this type of system is often exploited by spammers. Open relay is also known as an open relay server, insecure relay, third-party relay, open mail relay and spam relay.

## To perform SMTP open relay, in kali:

- msf console
- use auxiliary/scanner/smtp/smtp\_relay
- show options
- set RHOSTS ip address
- show options
- run

```
kali-linux-2021.1-virtual-machine-amd64 - VMware Workstation Player (Non-commercial use only)
Player ▾ | [Icons] | root@kali: /home/kali | 04:38 AM | 43% | [System Icons]
File Actions Edit View Help
root@kali: /home/kali

Code: 00 00 00 00 M3 T6 SP L0 IT FR 4M 3W 0H K1 V3 R5 L0 NS 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic! Attempted to kill the idle task!
to prevent race - not logging

-[ metasploit v6.0.0-dev ]
+ --[ 2172 exploits - 1138 auxiliary - 360 post ]
+ --[ 292 payloads - 45 encoders - 10 nops ]
+ --[ 8 evasion ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search

msf6 >
msf6 > use auxiliary/scanner/smtp/smtp_relay
msf6 auxiliary(scanner/smtp/smtp_relay) > show options

Module options (auxiliary/scanner/smtp/smtp_relay):



| Name     | Current Setting    | Required | Description                                                                       |
|----------|--------------------|----------|-----------------------------------------------------------------------------------|
| EXTENDED | false              | yes      | Do all the 16 extended checks                                                     |
| MALFROM  | sender@example.com | yes      | FROM address of the e-mail                                                        |
| MAILTO   | target@example.com | yes      | TO address of the e-mail                                                          |
| RHOSTS   |                    | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file::path' |
| RPORT    | 25                 | yes      | The target port (TCP)                                                             |
| THREADS  | 1                  | yes      | The number of concurrent threads (max one per host)                               |



msf6 auxiliary(scanner/smtp/smtp_relay) > set RHOSTS 192.168.101.129
RHOSTS => 192.168.101.129
msf6 auxiliary(scanner/smtp/smtp_relay) > run

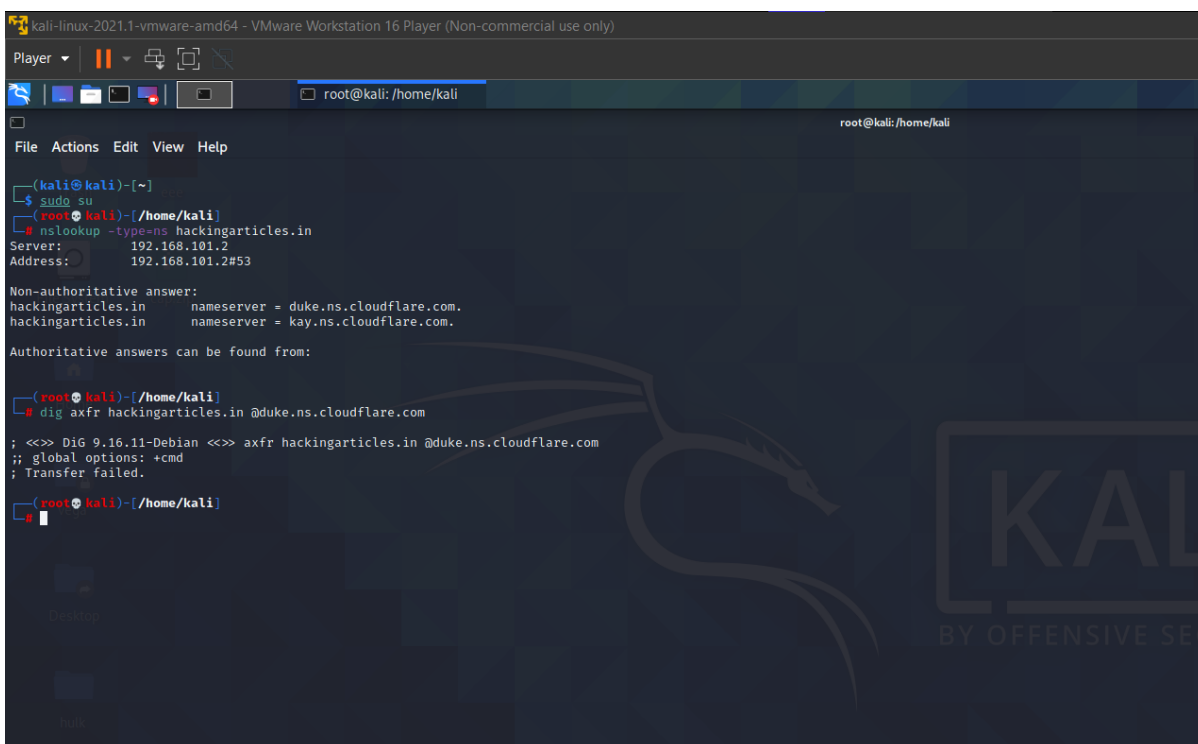
[*] 192.168.101.129:25 - SMTP 220 metaspoitable.localdomain ESMTP Postfix (Ubuntu)xkd'svda
[*] 192.168.101.129:25 - No relay detected
[*] 192.168.101.129:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_relay) >
```

## 2. Check for zone transfers

A zone transfer usually occurs when you bring up a new DNS server as a secondary DNS server. A full transfer of all the zone information will take place in order to replicate the already existing records for that zone. This is a time-consuming and resource-intensive process. Thus, incremental DNS transfers were developed. In the Incremental Transfer, the server retrieves only the resource records that have changed within a zone so that it remains synchronized with the primary DNS server. When using incremental transfer the SOA record is compared to see whether any changes have been made. If the primary name server has a higher SOA version number than the secondary name server then a zone transfer will be initiated.

**To perform zone transfer, in kali:**

- nslookup -type=ns hackingarticles
- dig axfr @nsztml.digi.ninja zonetransfer.me
- dnsenum zonetransfer.me
- sudo su
- dnsrecon -d zonetransfer.me

A screenshot of a Kali Linux terminal window running inside a VMware Workstation 16 Player. The terminal shows a user switching to root with 'sudo su' and then running 'nslookup -type=ns hackingarticles.in'. The output shows the server IP as 192.168.101.2 and the address as 192.168.101.2#53. It also shows non-authoritative answers for 'hackingarticles.in' with nameservers 'duke.ns.cloudflare.com' and 'kay.ns.cloudflare.com'. The user then runs 'dig axfr hackingarticles.in @duke.ns.cloudflare.com', which results in a 'Transfer failed' message. The terminal has a dark theme with a Kali Linux logo watermark in the background.

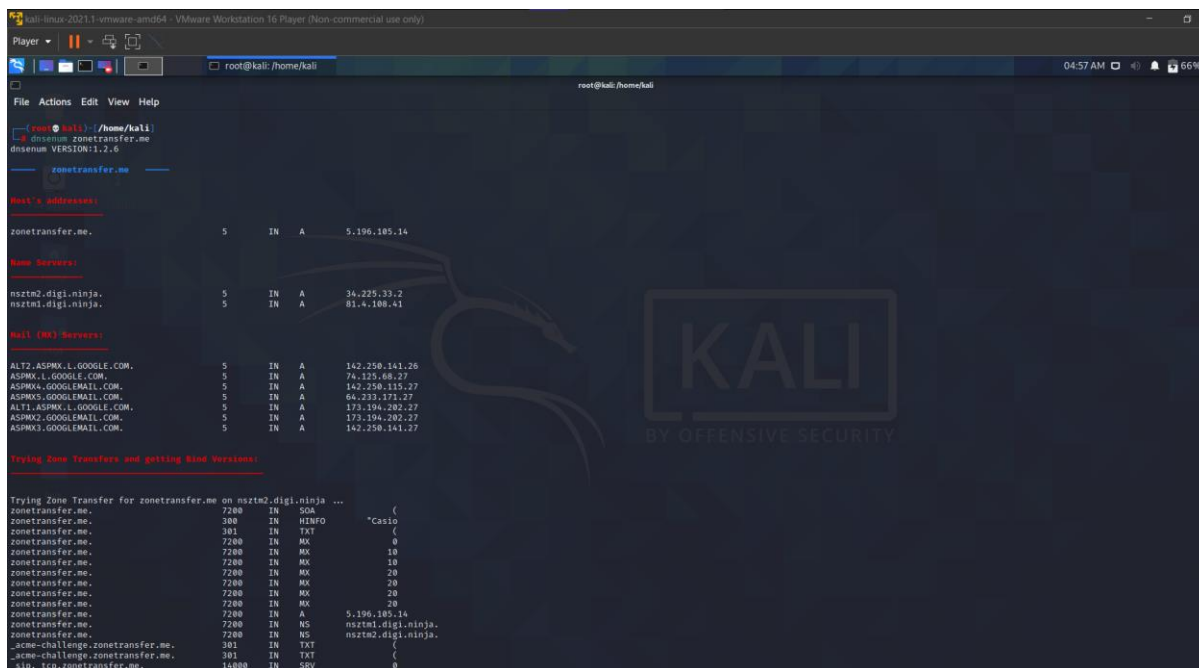
```
kali-linux-2021.1-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali
(kali@kali)~$ sudo su
(root@kali)~/home/kali$ nslookup -type=ns hackingarticles.in
Server:      192.168.101.2
Address:     192.168.101.2#53

Non-authoritative answer:
hackingarticles.in    nameserver = duke.ns.cloudflare.com.
hackingarticles.in    nameserver = kay.ns.cloudflare.com.

Authoritative answers can be found from:

(root@kali)~/home/kali$ dig axfr hackingarticles.in @duke.ns.cloudflare.com
; <<>> DiG 9.16.11-Debian <<>> axfr hackingarticles.in @duke.ns.cloudflare.com
;; global options: +cmd
;; Transfer failed.

(root@kali)~/home/kali$
```



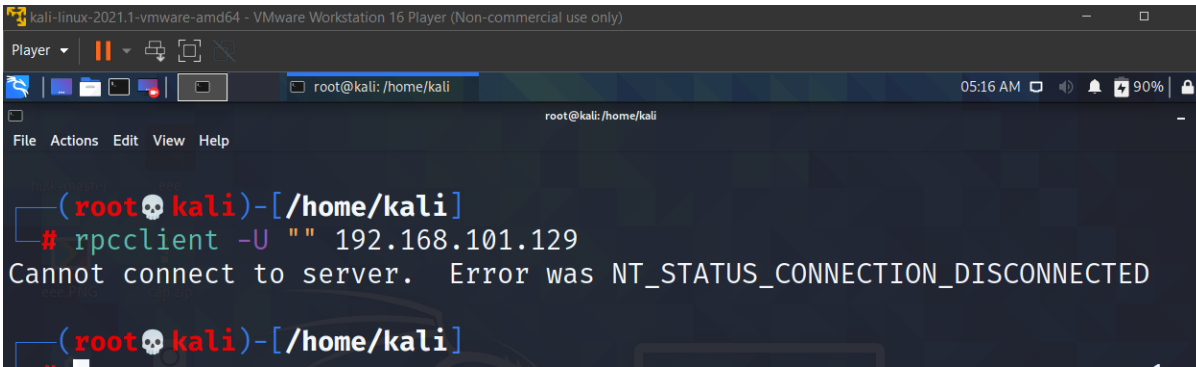
### 3.Perform NetBIOS enumeration

NetBIOS names are used to identify network devices over TCP/IP (Windows). The name must be a unique on a network, limited to 16 characters where 15 characters are used for the device name and the 16th character is reserved for identifying the type of service running or name record type. Short names are automatically and transparently padded to 16 characters. NetBIOS-over-TCP/IP (NBT) can implement a central repository, or Name Service, that records all name registrations. An application that wants to register a name would contact the name server and enquire whether the name is already registered, using a "Name Query" packet. The name server returns a negative response if the name is not already in the database, indicating that it is available. The Name Service, as specified in RFCs 1001 and 1002, is called NetBIOS Naming Service or NBNS. Microsoft WINDS is an implementation of NBNS. To start a session or to send a datagram to a particular host rather than to broadcast the datagram, NBT will have to determine the IP address of the host with a given NetBIOS name, this is done by broadcasting a "Name Query" packet, and /or sending it to the NetBIOS name server. The response will have the IP address of the host with that name.

## To perform NetBIOS enumeration, in kali:

- `sudo su`
- `rpcclient -u "" ipaddress`
- `querydomaininfo`
- `enumdomusers`

- queryuser (name)

A screenshot of a Kali Linux terminal window running inside a VMware Workstation 16 Player. The terminal shows a root user at the kali machine in the /home/kali directory. The user enters the command `rpcclient -U "" 192.168.101.129`. The output of the command is "Cannot connect to server. Error was NT\_STATUS\_CONNECTION\_DISCONNECTED". The terminal window has a dark theme and a menu bar with File, Actions, Edit, View, and Help. The VMware window title is "kali-linux-2021.1-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)".

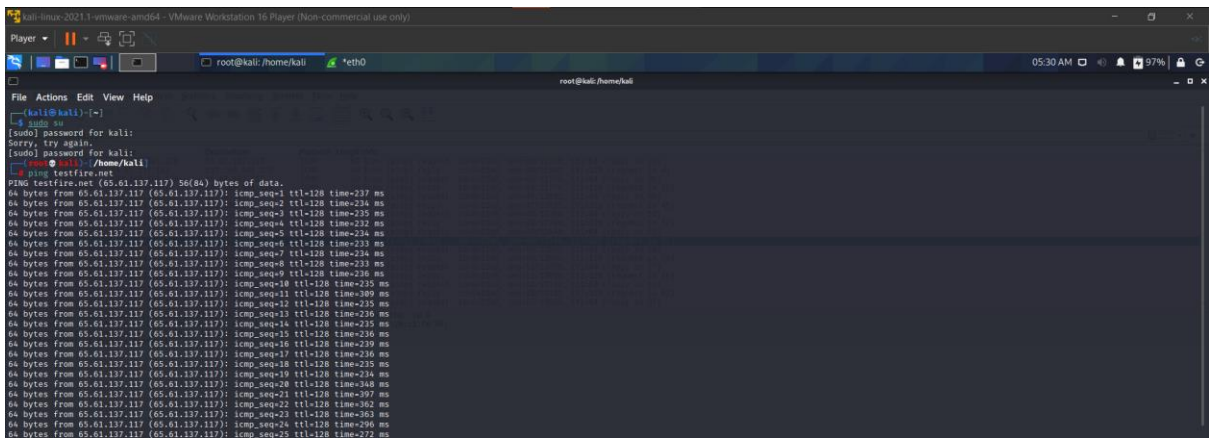
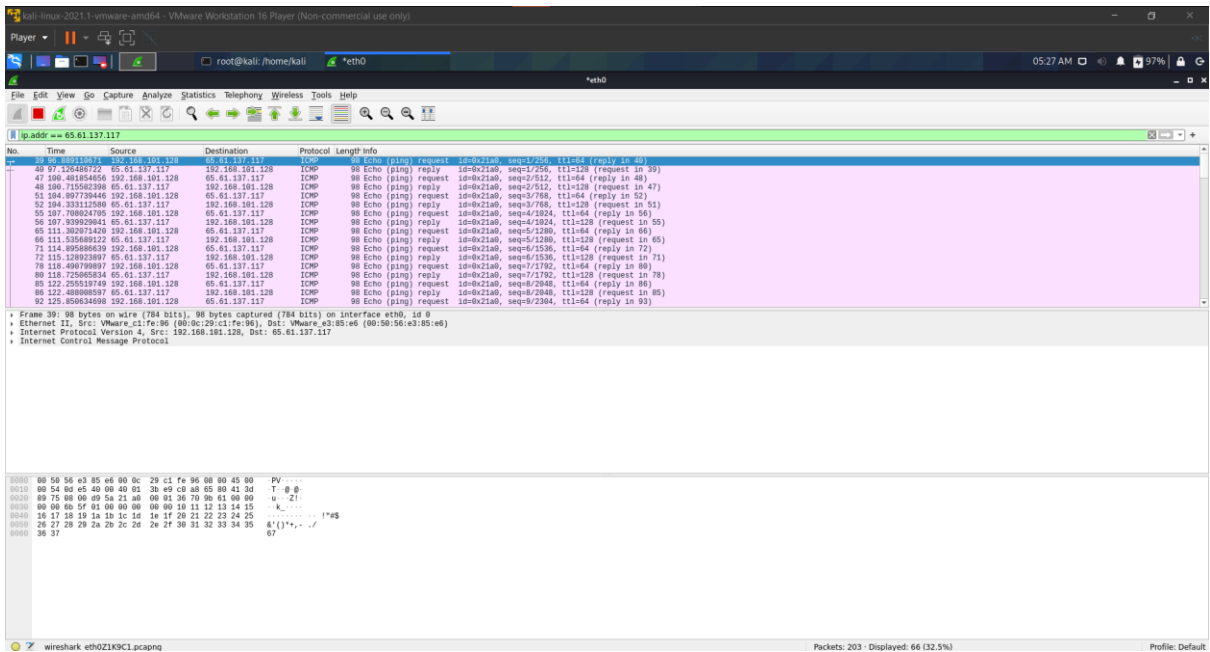
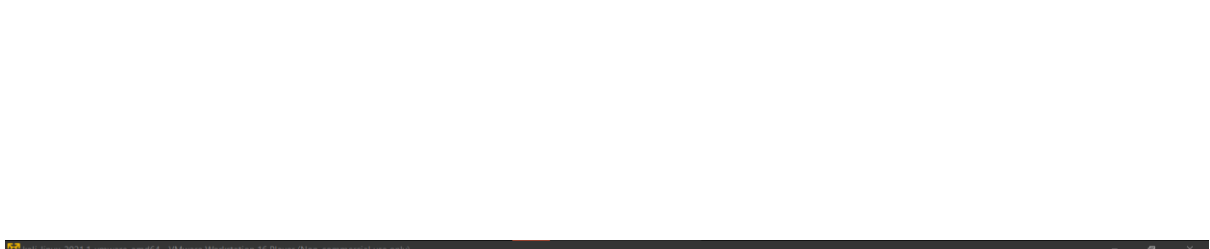
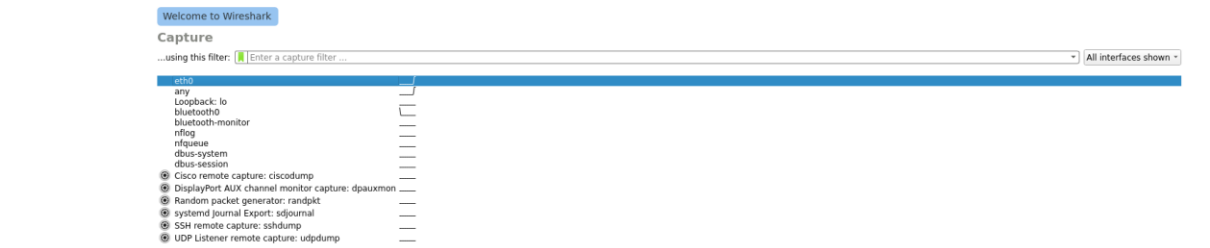
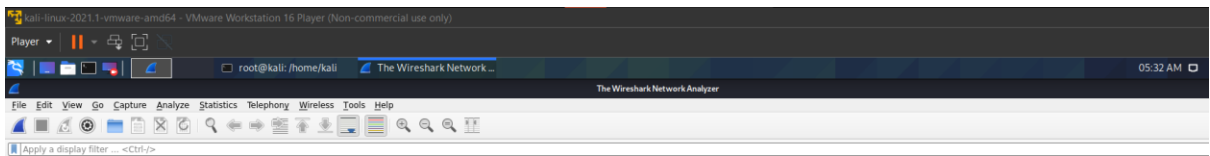
```
kali-linux-2021.1-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home/kali
05:16 AM 90%
File Actions Edit View Help
root@kali: /home/kali
(root@kali)-[/home/kali]
# rpcclient -U "" 192.168.101.129
Cannot connect to server. Error was NT_STATUS_CONNECTION_DISCONNECTED
(root@kali)-[/home/kali]
```

## 4.Sniff the data of any application using wire-shark

Wireshark is an open-source, free network packet analyzer, used to capture and analyze network traffic in real-time. It's considered one of the most essential network security tools by ethical hackers. In short, with Wireshark you can capture and view data traveling through your network. Many people gravitate towards Wireshark's robust GUI, used for packet capturing and analysis. Packet Analyzers operate by allowing a user to put network interface controllers (NIC's) in promiscuous mode in order to view and capture network traffic. For instance, packets that are captured through Wireshark are filtered into data streams, paths, protocols, and IP addresses to be analyzed and studied in greater detail.

**To use whire shark in system hacking, in kali:**

- sudo su
- ping testfire.net
- eth0 packets
- open whire shark packets



## 5.Perform DOs Attack using metasploit framework

Typically, a Penetration Testing exercise is focused on identifying the gaps in security rather than harming a system. This is a key feature that separates a real attacker from an authorized Penetration Tester. Real hackers don't follow the rules and are not concerned about interrupting business if it can improve their situation. In some cases, a hacker is looking to create any form of negative impact on a target, including taking down critical systems. For this reason, it makes sense in some cases to test systems for the risk Denial of Service(DoS) type attacks. This is commonly termed as stress testing your Internet facing services. The most common DoS attack involves flooding a target with external communication requests. This overload prevents the resource from responding to legitimate traffic, or slows its response so significantly that it is rendered unavailable. DoS attacks can target system resources (IE disk space, bandwidth, and so on), configuration information (IE remove route tables), state information (TCP session resetting), or anything that can harm system operation.

**To use Dos attackusing Metasploit framework in system hacking, in kali:**

- `sudo su`
- `msfconsole`
- `use auxiliary/dos/tcpsynflood`
- `show options`
- `set RHOSTS (ip address from comant prompt )`
- `show options`
- `run`
- `open whiteshark`

