

ASSIGNMENT_2

KALI_LINUX_TOOL_EXPLORATION

1. Nmap - Network Mapping:

Nmap is a free and open-source network discovery and security auditing utility. It is used to scan large networks to identify hosts and services, and to detect vulnerabilities.

```
(root@kali)-[~]
# nmap -F vtop.vit.ac.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 12:00 EDT
Nmap scan report for vtop.vit.ac.in (136.233.9.22)
Host is up (0.038s latency).
rDNS record for 136.233.9.22: 136.233.9.22.static.jio.com
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.12 seconds
```

2. Nikto Tool:

The Nikto web server scanner is a security tool that will test a web site for thousands of possible security issues. Including dangerous files, mis-configured services, vulnerable scripts and other issues. It is open source and structured with plugins that extend the capabilities. These plugins are frequently updated with new security checks.

```
(root@kali)-[~]
# nikto -h vtop.vit.ac.in
- Nikto v2.5.0

+ Target IP: 136.233.9.22
+ Target Hostname: vtop.vit.ac.in
+ Target Port: 80
+ Start Time: 2023-10-09 12:05:37 (GMT-4)

+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://
+ /: The X-Content-Type-Options header is not set. This could allow the user ag
ing-content-type-header/
+ Root page / redirects to: https://vtop.vit.ac.in/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

3. Metasploit:

Metasploit is an open-source penetration testing framework that provides a wide range of tools and exploits for attacking systems. It can be used to exploit vulnerabilities in operating systems, applications, and services.


```

(root@kali)-[~]
# evil-winrm -i vtop.vit.ac.in

Evil-WinRM shell v3.5

Error: missing argument: user

Usage: evil-winrm -i IP -u USER [-s SCRIPTS_PATH] [-e EXES_PATH] [-P PORT] [-p F
  -S, --ssl                               Enable ssl
  -c, --pub-key PUBLIC_KEY_PATH           Local path to public key certificate
  -k, --priv-key PRIVATE_KEY_PATH         Local path to private key certificate
  -r, --realm DOMAIN                      Kerberos auth, it has to be set also in /et
  -s, --scripts PS_SCRIPTS_PATH          Powershell scripts local path
      --spn SPN_PREFIX                    SPN prefix for Kerberos auth (default HTTP)
  -e, --executables EXES_PATH             C# executables local path
  -i, --ip IP                             Remote host IP or hostname. FQDN for Kerber
  -U, --url URL                            Remote url endpoint (default /wsman)
  -u, --user USER                         Username (required if not using kerberos)
  -p, --password PASS                     Password
  -H, --hash HASH                          NTHash
  -P, --port PORT                         Remote host port (default 5985)
  -V, --version                           Show version
  -n, --no-colors                         Disable colors
  -N, --no-rpath-completion               Disable remote path completion
  -l, --log                               Log the WinRM session
  -h, --help                             Display this help message

```

6. Ncrack:

Ncrack is a high-speed network authentication cracking tool. It was built to help companies secure their networks by proactively testing all their hosts and networking devices for poor passwords. Security professionals also rely on Ncrack when auditing their clients.

```

(root@kali)-[~]
# ncrack -h has you

Ncrack 0.7 ( http://ncrack.org )
Usage: ncrack [Options] {target and service specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iX <inputfilename>: Input from Nmap's -oX XML output format
  -iN <inputfilename>: Input from Nmap's -oN Normal output format
  -iL <inputfilename>: Input from list of hosts/networks
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
SERVICE SPECIFICATION:
  Can pass target specific services in <service>://target (standard) notation or
  using -p which will be applied to all hosts in non-standard notation.
  Service arguments can be specified to be host-specific, type of service-specific
  (-m) or global (-g). Ex: ssh://10.0.0.10,at=10,cl=30 -m ssh:at=50 -g cd=3000
  Ex2: ncrack -p ssh,ftp:3500,25 10.0.0.10 scanme.nmap.org google.com:80,ssl

```