

COMPLETE ETHICAL HACKING COURSE

PROF. SUNIL K. GUPTA

ETHICAL HACKER / CYBER SECURITY SPECIALIST

Vulnerability Assessment : Nikto Tool

- Nikto is used to find Vulnerabilities in a web server .

1. Nikto Command –

- `nikto -h www.xyz.com -Tuning 1`
- `Nikto -h www.xyz.com`

Vulnerability Analysis : Nikto

```
Applications File Edit View VM Tabs Help
root@kali:~# nikto -h http://www.psuconnect.in/ -Tuning 1
Nikto v2.1.6
-----
+ Target IP: 192.185.168.219
+ Target Hostname: www.psuconnect.in
+ Target Port: 80
+ Start Time: 2017-03-06 04:14:55 (GMT-5)
-----
+ Server: nginx/1.10.3
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Entry '/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/psuadmin/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
^Croot@kali:~# clear
root@kali:~# nikto -h http://hongkonggas.co.th/
- Nikto v2.1.6
-----
+ ERROR: Cannot resolve hostname 'hongkonggas.co.th'
+ 0 host(s) tested
root@kali:~# nikto -h http://hongtonggas.co.th/
- Nikto v2.1.6
-----
+ ERROR: Cannot resolve hostname 'hongtonggas.co.th'
+ 0 host(s) tested
root@kali:~# nikto -h http://www.bible-history.com/
- Nikto v2.1.6
-----
+ Target IP: 54.201.8.54
+ Target Hostname: www.bible-history.com
+ Target Port: 80
+ Start Time: 2017-03-06 04:20:37 (GMT-5)
-----
+ Server: Apache/2.4.25 (Amazon) PHP/5.5.38
```

COMPLETE ETHICAL HACKING COURSE

Thank you

PROF. SUNIL K. GUPTA
ETHICAL HACKER / CYBER SECURITY SPECIALIST