

Scan Tools Profile Help

Target: 93.186.225.194 Profile: Intense scan

Command: nmap -T4 -A -v 93.186.225.194

Hosts		Services				
OS	Host	Port	Protocol	State	Service	Version
	192.168.0.1	80	tcp	open	http	Cloudflare http proxy
	188.114.99.224	443	tcp	open	http	Cloudflare http proxy
	104.21.51.216	8080	tcp	open	http	Cloudflare http proxy
	93.186.225.194	8443	tcp	open	http	Cloudflare http proxy
	lu-in-f198.1e100.					

HLTV.org

Присутствуют порты 80, 443, 8080, 8443

Zenmap

Scan Tools Profile Help

Target: 93.186.225.194 Profile: Intense scan

Command: nmap -T4 -A -v 93.186.225.194

Hosts		Services				
OS	Host	Port	Protocol	State	Service	Version
	192.168.0.1	80	tcp	open	http	Cloudflare http proxy
	188.114.99.224	443	tcp	open	https	cloudflare
	104.21.51.216	8080	tcp	open	http	Cloudflare http proxy
	93.186.225.194	8443	tcp	open	https-alt	cloudflare
	lu-in-f198.1e100.					

Cross.bet

Присутствуют порты 80, 443, 8080, 8443

Zenmap

Scan Tools Profile Help

Target: 93.186.225.194 Profile: Intense scan

Command: nmap -T4 -A -v 93.186.225.194

Hosts Services

OS	Host
Ubuntu	192.168.0.1
Windows	188.114.99.224
Windows	104.21.51.216
Windows	93.186.225.194
Windows	lu-in-f198.1e100.

Nmap Output Ports / Hosts Topology Host Details Scans

	Port	Protocol	State	Service	Version
Green circle	80	tcp	open	http	kittenx
Green circle	443	tcp	open	https	kittenx

Vk.com

Присутствуют порты 80, 443

The screenshot shows the Zmap interface with the following configuration:

- Scan menu is open.
- Target: 93.186.225.194
- Profile: Intense scan
- Command: nmap -T4 -A -v 93.186.225.194

The main window displays the following table:

Hosts		Services				
OS	Host	Port	Protocol	State	Service	Version
Windows	192.168.0.1	80	tcp	open	http	gws
Windows	188.114.99.224	443	tcp	open	https	gws
Windows	104.21.51.216					
Windows	93.186.225.194					
Windows	lu-in-f198.1e100.					

Youtube.com

Присутствуют порты 80, 443