

Scanning Network Using Zenmap

The screenshot shows the Zenmap application window. At the top, there's a menu bar with 'Сканирование', 'Инструменты', 'Профиль', and 'Помощь'. Below the menu, there's a header area with 'Цель' (Target) set to '192.168.0.1', 'Профиль' (Profile) set to 'Intense scan', and buttons for 'Сканирование' (Scan) and 'Отмена' (Cancel). A 'Команда' (Command) field contains 'nmap -T4 -A -v 192.168.0.1'.

The main interface is divided into two main sections. On the left is a sidebar with 'Узлы' (Nodes) and 'Сервисы' (Services) tabs. Under 'Узлы', there's a list of nodes, including '192.168.0.1'. The right section contains a 'Вывод Nmap' (Nmap Output) tab, which displays the results of the scan in a terminal-like format. The output includes port scan results, service version detection, and various host details.

The Nmap output shows the following information:

- PORT STATE SERVICE VERSION**
- 22/tcp open ssh** Dropbear sshd 2012.55 (protocol 2.0)
- ssh-hostkey:
 - 1024 07d6bb6ffb6f46fb715d8093d77aa623 (DSA)
 - 1039 11d23290d6e54e3828c03179a10e18c0 (RSA)
- 53/tcp open tcpwrapped**
- 80/tcp open http** TP-LINK TD-W8968 http admin
- http-methods:
 - Supported Methods: GET POST
 - http-title: Site doesn't have a title (text/html; charset=utf-8).
- 1900/tcp open upnp** Portable SDK for UPnP devices 1.6.19 (Linux 2.6.36; UPnP 1.0)
- MAC Address:** 68:FF:7B:A7:F5:34 (Tp-link Technologies)
- Device type:** general purpose
- Running:** Linux 2.6.X
- OS CPE:** cpe:/o:linux:linux_kernel:2.6
- OS details:** Linux 2.6.23 - 2.6.38
- Uptime guess:** 11.582 days (since Fri Dec 23 12:16:15 2022)
- Network Distance:** 1 hop
- TCP Sequence Prediction:** Difficulty=195 (Good luck!)
- IP ID Sequence Generation:** All zeros
- Service Info:** OS: Linux; Device: WAP; CPE: cpe:/o:linux:linux_kernel, cpe:/h:tp-link:td-w8968, cpe:/o:linux:linux_kernel:2.6.36

Below the port scan results, there's a 'TRACEROUTE' section showing the path to the target:

HOP	RTT	ADDRESS
1	3.90 ms	192.168.0.1

At the bottom, there's an 'NSE' (Nmap Scripting Engine) section showing the results of post-scan scripts:

```

NSE: Script Post-scanning.
Initiating NSE at 02:14
Completed NSE at 02:14, 0.00s elapsed
Initiating NSE at 02:14
Completed NSE at 02:14, 0.00s elapsed
Initiating NSE at 02:14
Completed NSE at 02:14, 0.00s elapsed
  
```

The bottom of the window features a 'Фильтр узлов' (Filter nodes) button.