Acquiring Intel from Other Enumeration Techniques

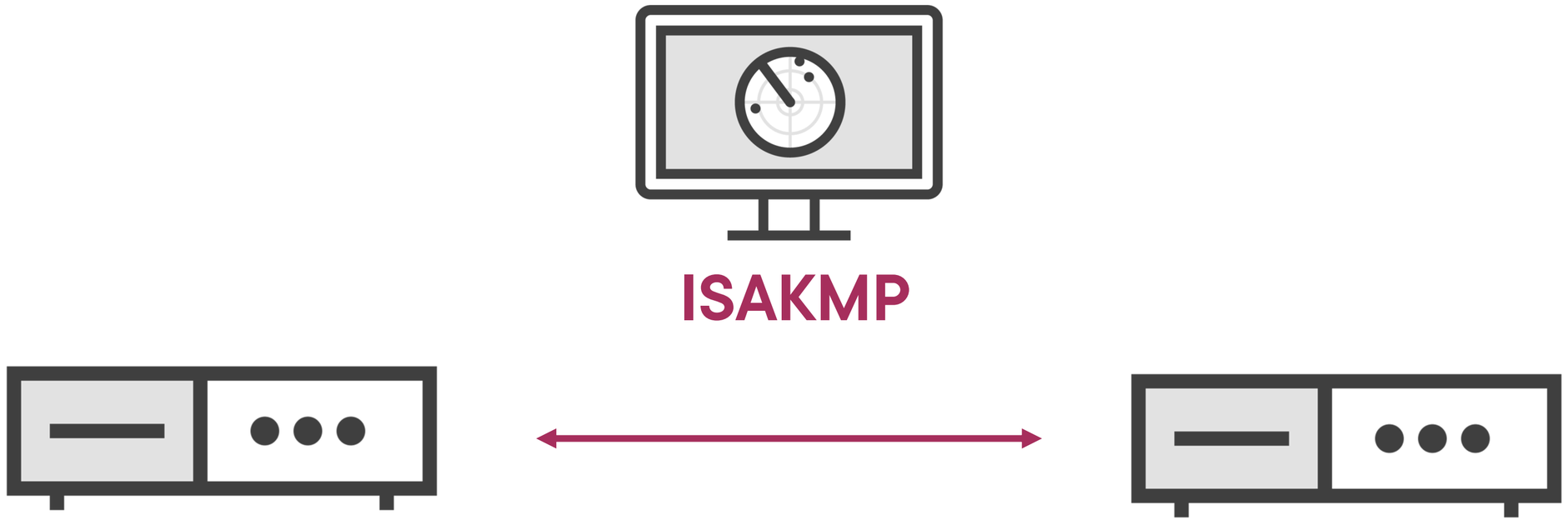
Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

YES! I am invincible!

Boris Grishenko

IPSec Enumeration



Internet Security Association and Key Management Protocol

SA = Security Association

IPSec Enumeration

```
Nmap –sU –p 500 <targetIP>
```

```
Ike-scan –M <targetIP>
```

https://github.com/royhills/ike-scan

VoIP Enumeration

VoIP Enumeration

Session Initiation Protocol (SIP)

UDP or TCP ports

2000, 2001, 5050, and 5061

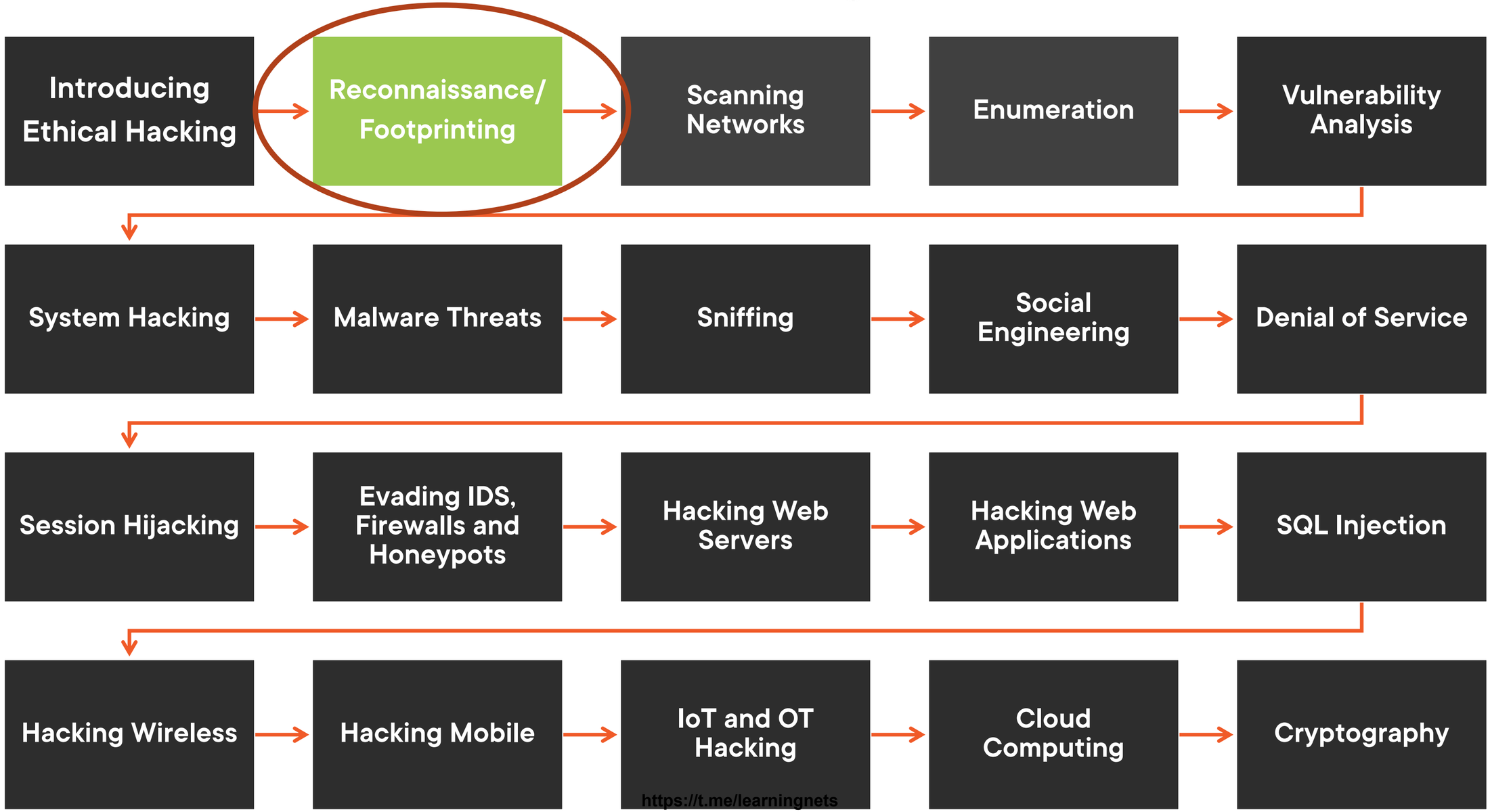
VoIP Enumeration Tools

SIPVicious

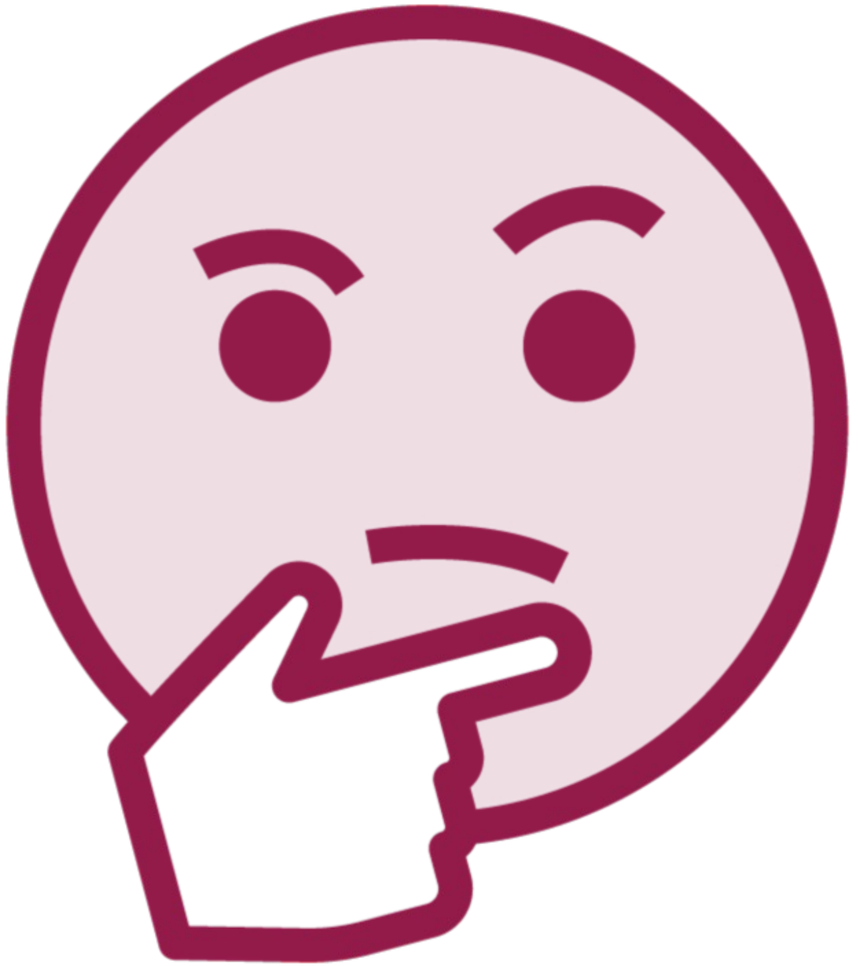
Svmap

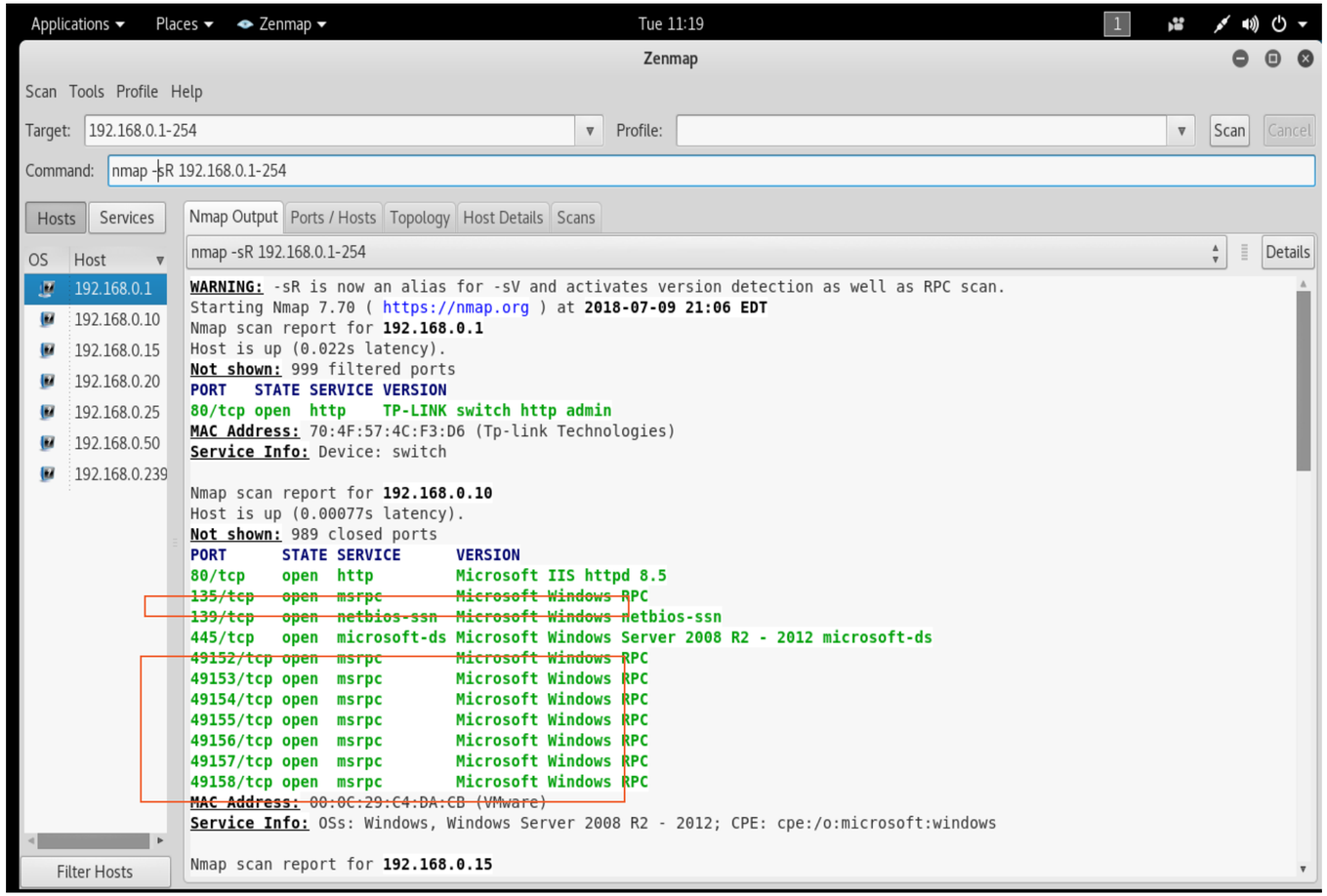
Google Hacking

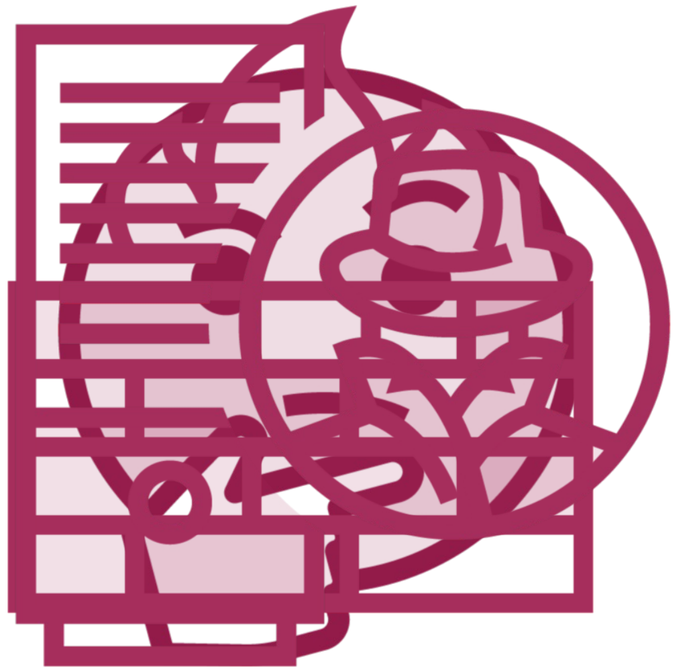
Ethical Hacking Series



Using RPC Enumeration





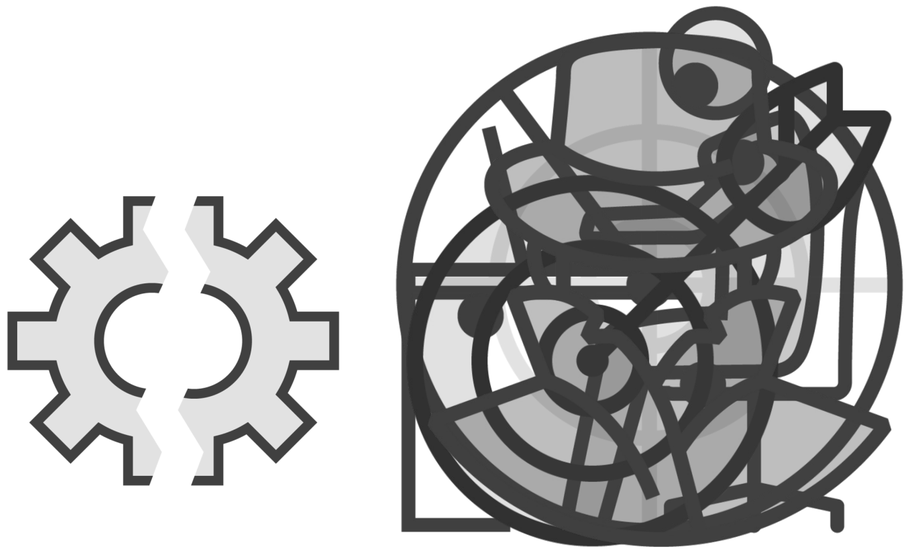


nmap -sR 192.168.0.1-254

Using Telnet, SMB, FTP, and More

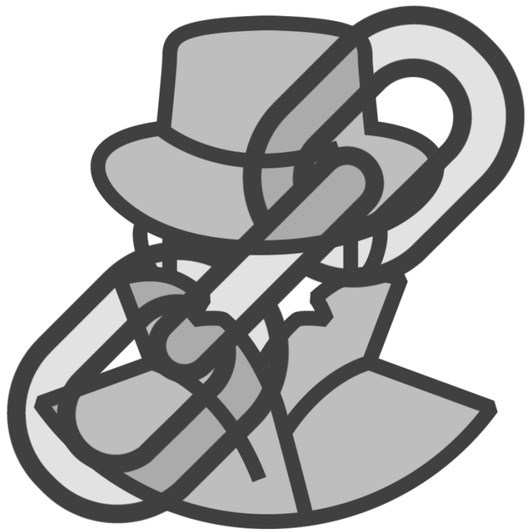
Using Telnet, SMB, FTP, and More

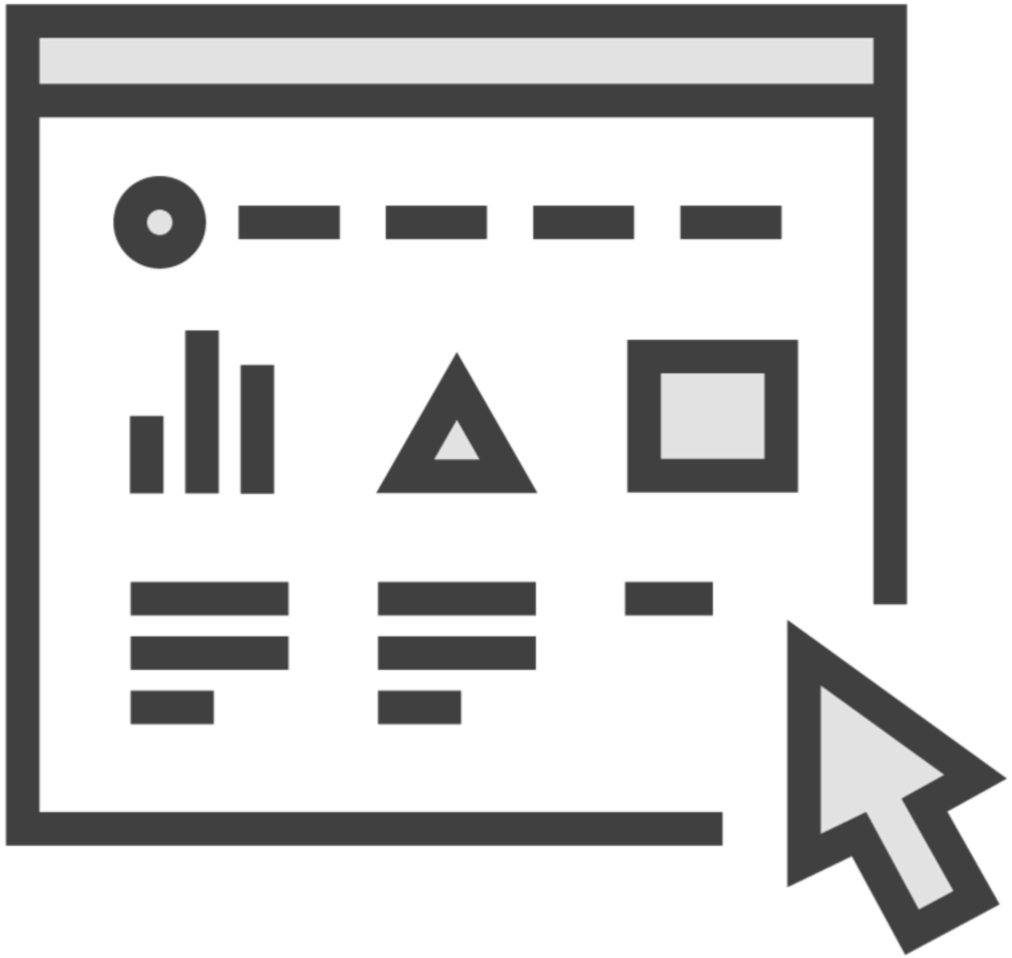
- **Telnet port 23 (nmap –p 23 <target>)**
- **SMB port 445 (nmap –p 445 –A <target>)**
- **FTP port 21 (nmap –p 21 <target>)**
- **TFTP port 69**

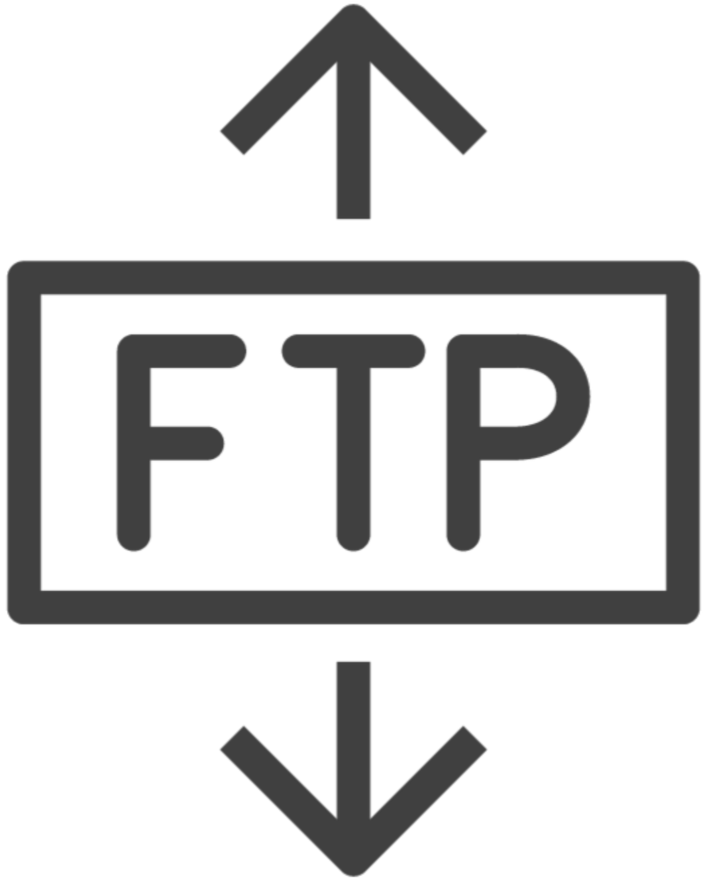


Using Telnet, SMB, FTP, and More

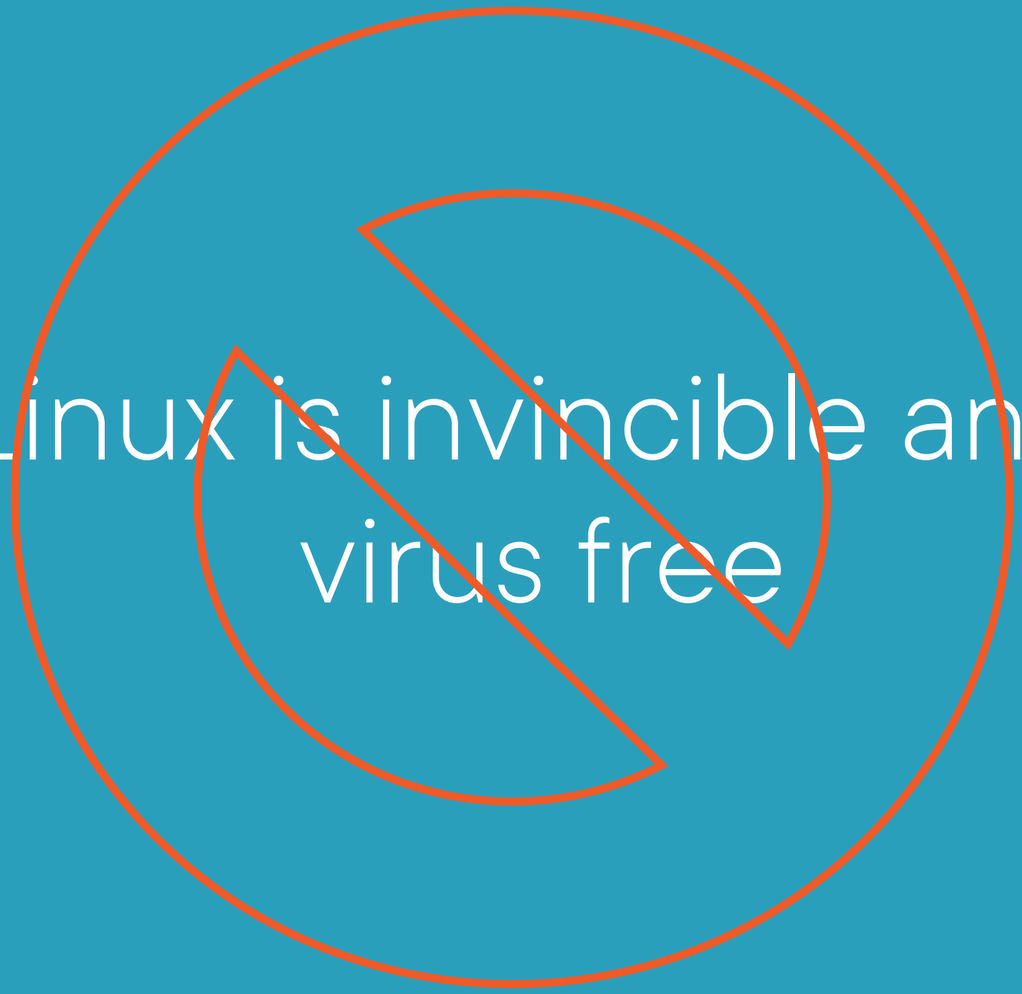
- **Telnet port 23 (nmap –p 23 <target>)**
- **SMB port 445 (nmap –p 445 –A <target>)**
- **FTP port 21 (nmap –p 21 <target>)**
- **TFTP port 69**
- **BGP port 179**







Why Is Linux Considered Secure?



The moment you feel invincible is when you need to slow down and take a look at what you're doing and what you're using, as no person, system, process, or platform is invincible.

Dale Meredith

Demo

Common commands to enumerate

Learning Check

Learning Check

- **VoIP**
- **Ike-scan**
- **enum4linux**
- **/etc/shadow**

Up Next:
Discovering Enumeration Countermeasures