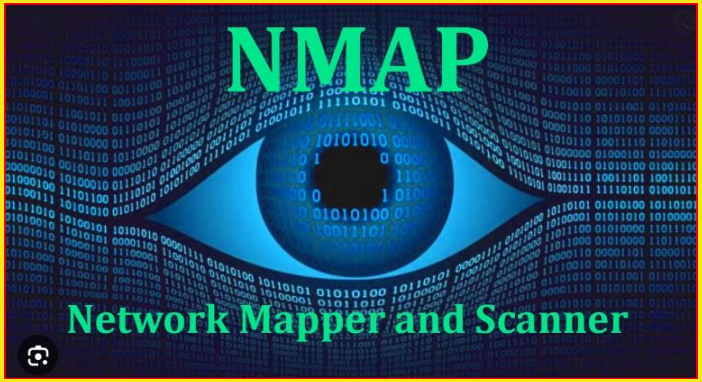
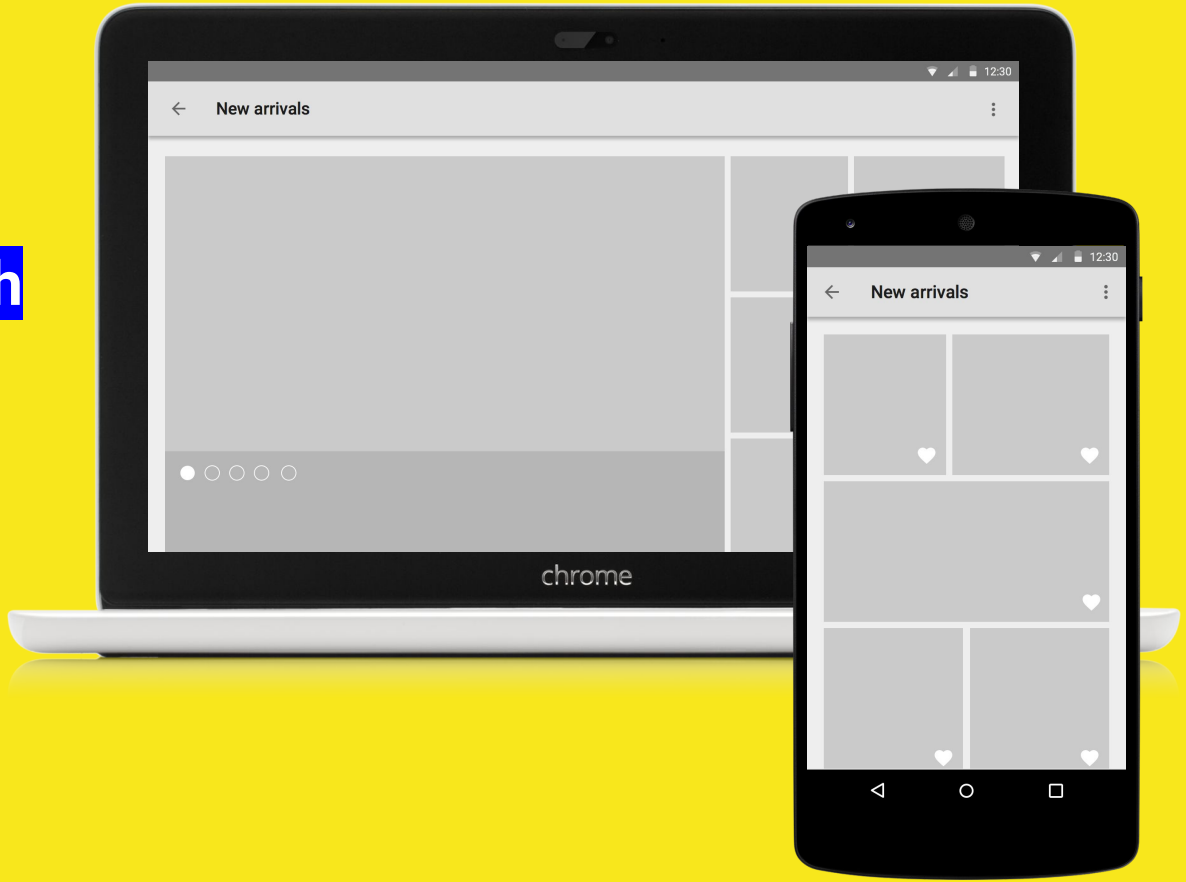
BootCon: Nmap Project

– – –

Topic:

“Network Scanning with Nmap to access”





ABIB SUBBA

Project 5 BootCon Presentation

“Network Scanning with Nmap to access”

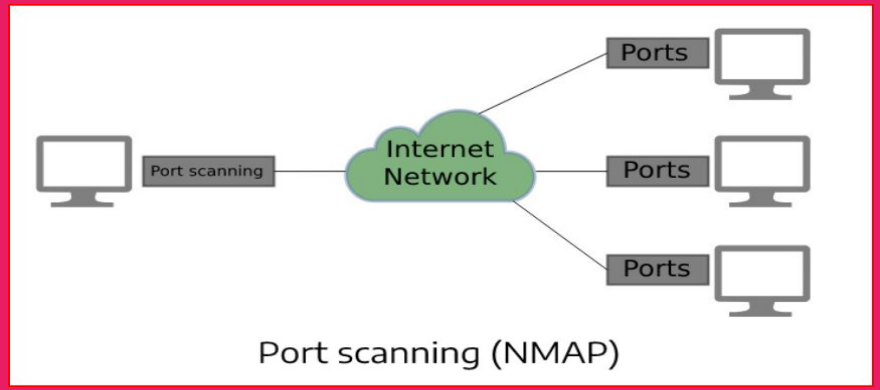
About Topic Selection

- Relevance to Current Threat Landscape
- Practical Application for Security Professionals
- Open-Source and Widely Adopted
- Integration with Widely Used OS
- Aligns with BootCon's Focus on Practical Security Solutions

Networking security concepts applied

- Port Scanning for Vulnerability Assessment.
- Service Version Detection.
- Proper authorization and adherence to legal standards.
- Operating System for comprehensive network scanning.
- Scripting Engine for Automation.
- Network Segmentation and Firewall Configuration.

Research steps taken



Port scanning (NMAP)

- Literature Review on Nmap and Network Scanning
- Analysis of Windows 10 Integration with Nmap
- Identification of Security Best Practices
- Selection of Scanning Techniques and Methodologies
- Testing and Validation

Practical Demonstration steps

Scan Specific Ports (80, 443)

Scan Range of Ports (1-200)

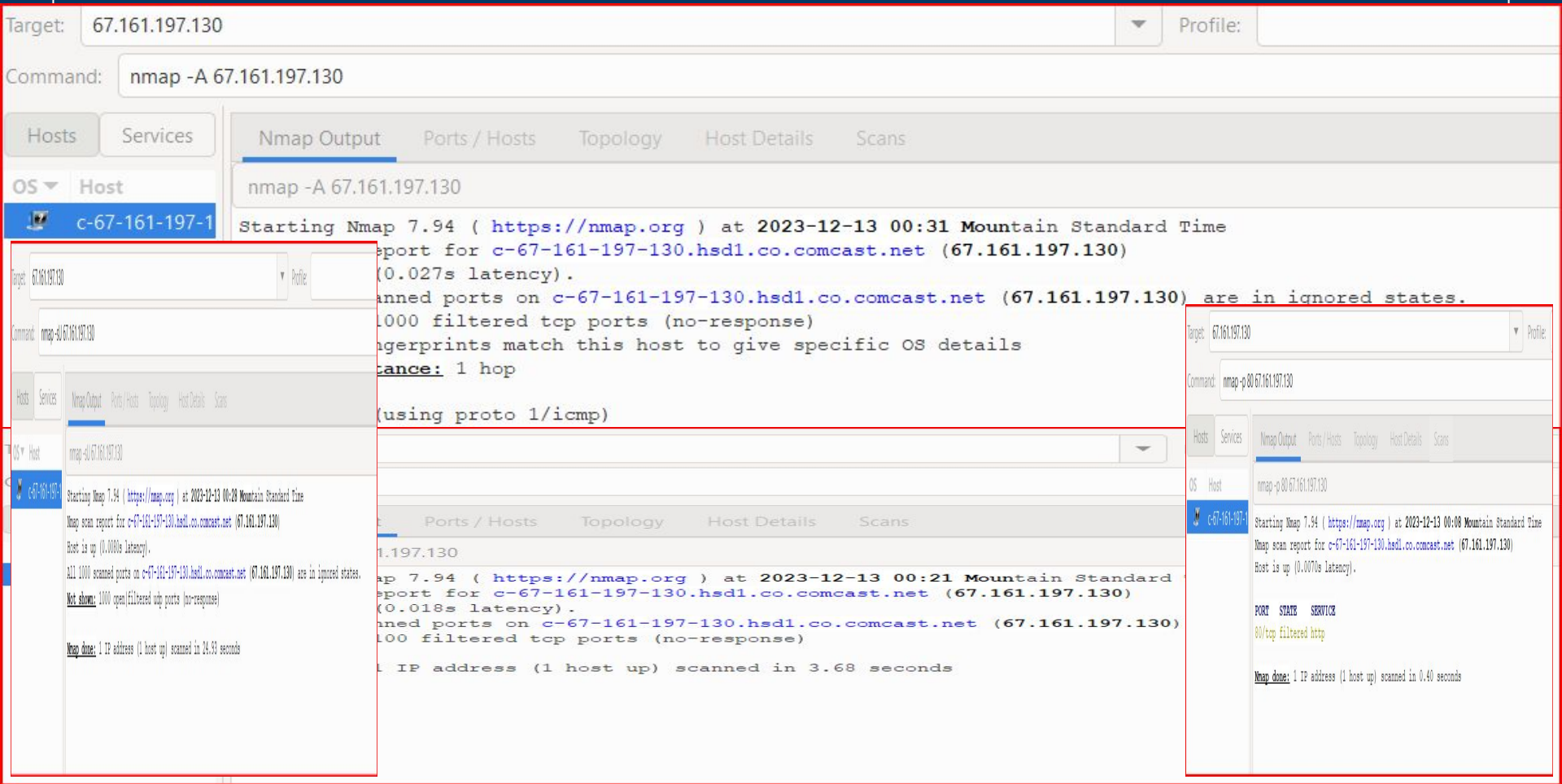
Scan Most Common Ports

Switch IP Address and Scan

TCP Scan UDP Ports

Detect Operating System

NETWORK NMAPPER & SCANNER SCREENSHOTS



Ubuntu Screenshots

```
Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
sysadmin@vm-image-ubuntu-dev-1:~$ nmap -F 67.161.197.130 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-15 03:04 UTC
Nmap scan report for c-67-161-197-130.hsd1.co.comcast.net (67.161.197.130)
Host is up.
All 100 scanned ports on c-67-161-197-130.hsd1.co.comcast.net (67.161.197.130) a
re filtered

Nmap done: 1 IP address (1 host up) scanned in 21.07 seconds
sysadmin@vm-image-ubuntu-dev-1:~$ nmap google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-15 03:04 UTC
Nmap scan report for google.com (142.250.189.206)
Host is up (0.0027s latency).
Other addresses for google.com (not scanned): 2607:f8b0:4005:80d::200e
rDNS record for 142.250.189.206: sfo03s25-in-f14.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

```
sysadmin@vm-image-ubuntu-dev-1:~$ nmap -p 1-200 67.161.197.130 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-15 03:02 UTC
Nmap scan report for c-67-161-197-130.hsd1.co.comcast.net (67.161.197.130)
Host is up.
All 200 scanned ports on c-67-161-197-130.hsd1.co.comcast.net (67.161.197.130) a
re filtered

Nmap done: 1 IP address (1 host up) scanned in 41.09 seconds
sysadmin@vm-image-ubuntu-dev-1:~$ nmap -p 17 67.161.197.130 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-15 03:03 UTC
Nmap scan report for c-67-161-197-130.hsd1.co.comcast.net (67.161.197.130)
Host is up.

PORT   STATE    SERVICE
17/tcp filtered qotd

Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
sysadmin@vm-image-ubuntu-dev-1:~$ nmap -F 67.161.197.130 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-15 03:04 UTC
Nmap scan report for c-67-161-197-130.hsd1.co.comcast.net (67.161.197.130)
Host is up.
All 100 scanned ports on c-67-161-197-130.hsd1.co.comcast.net (67.161.197.130) a
re filtered
```

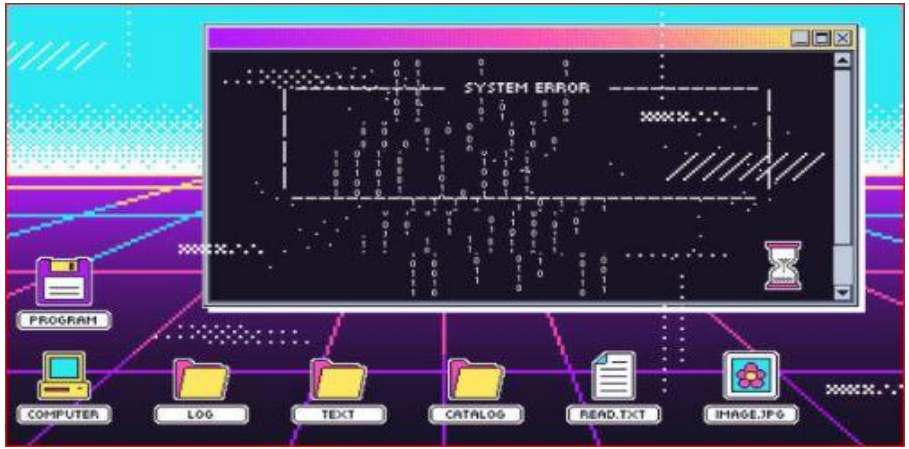
END GOAL:

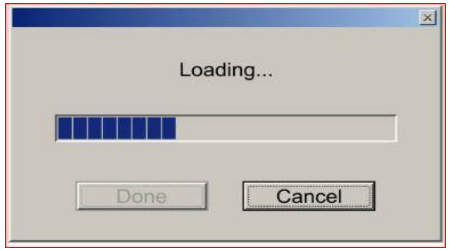
"Systematically scan, identify vulnerabilities, and implement best-practice security measures."

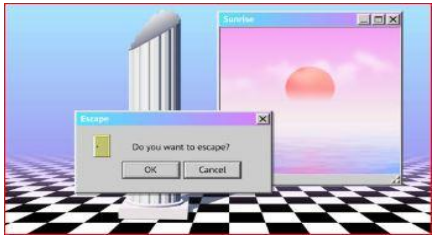
- Emphasize Best Practices
- Utilize Nmap's Features

- Analysis for Action
- Align with Cybersecurity Standards

Adapt to Best Security Practice Recommendations







Devices Used:

Windows 10 Operating System

Devices Used:

Network-Connected Devices

Summary of Device and Technology Usage

- Nmap Utilization
- Scanning Techniques
- Efficient Scanning with Windows 10
- Comprehensive Risk Analysis
- Proactive Security Measures

Conclusion

BootCon emphasizes practical skills. This presentation aims to leave attendees equipped with the knowledge and skills needed to implement effective Nmap Scan using advancing scanning techniques in their professional settings.

Q&A and Interactive Session:

- ???