DEFEND WORKSHOP

Izdihar

cyber673

PRACTICAL NMAP FOR ASSET DISCOVERY

```
# Basic network discovery scan
nmap -sn 192.168.0.0/24

# Detailed service detection scan
nmap -sV 192.168.0.0/24

# Output to file for documentation
nmap -sV 192.168.0.0/24 -oN scan_results.txt
```

PRACTICAL NMAP FOR ASSET DISCOVERY

Practical Tips:

- Look for unexpected open ports (22, 80, 443, 3389)
- Check for unauthorized services
- Compare against your inventory document

VULNERABILITY SCANNING WITH NUCLEI

What is Nuclei?

- Open-source vulnerability scanner
- Template-based detection approach
- Faster and more customizable than many commercial tools
- Perfect for SMEs and blue teams with limited resources

cyber673

VULNERABILITY SCANNING WITH NUCLEI

```
# Basic scan of a target
nuclei -u http://example.com -o results.txt

# Scan multiple targets
nuclei -l hosts.txt -o results.txt

# Scan with specific severity levels
nuclei -u http://example.com -severity critical,high

# Scan specific vulnerability types
nuclei -u http://example.com -tags cve,rce,oast
```

cyber673

VULNERABILITY SCANNING WITH NUCLEI

Interpreting Results:

- Focus on critical and high severity findings first
- Validate findings to eliminate false positives
- Prioritize internet-facing vulnerabilities
- Document and track remediation status

SECURITY CONFIGURATION ANALYSIS

File Locations to Check:

- Linux: /etc/ssh/sshd_config, /etc/passwd, crontabs
- Windows: Registry, scheduled tasks, startup items

Common Misconfigurations:

- Default credentials
- Password authentication enabled
- Excessive permissions
- Plaintext secrets in config files

SECURITY CONFIGURATION ANALYSIS

```
# Find files containing password strings
grep -r "password" --include="*.conf" /etc/
grep -r "key" --include="*.json" /home/

# Check SSH configuration
cat /etc/ssh/sshd_config | grep "PasswordAuthentication"
```

LOG ANALYSIS TECHNIQUES

Common Log Patterns to Look For:

- Failed login attempts in sequence (brute force)
- Suspicious IP addresses or geolocations
- Unusual access times
- Sensitive file access
- Command execution patterns

LOG ANALYSIS TECHNIQUES

```
# Count occurrences of IPs in logs
cat auth.log | grep "Failed password" | awk '{print $11}' | sort | uniq -c | sort -nr

# Find events within a timeframe
cat auth.log | grep "Apr 22" | grep "authentication failure"

# Detect unusual admin actions
cat auth.log | grep "sudo" | grep -v "user=root"
```

MALWARE IDENTIFICATION

Quick File Analysis:

```
# Check file type
file suspicious_file

# See strings inside a file
strings suspicious_file | less

# Calculate file hash for VirusTotal
sha256sum suspicious_file
```

MALWARE IDENTIFICATION

Red Flags:

- Executable files in unexpected locations
- Files with multiple extensions (.doc.exe)
- Base64-encoded scripts
- Obfuscated code

INCIDENT RESPONSE BASICS

Initial Response Steps:

- Document what's happening
- Contain the issue (isolate affected systems)
- Collect evidence before changes
- Determine impact and scope
- Remediate and recover

INCIDENT RESPONSE BASICS

Documentation Focus:

- Timestamps of all actions
- Systems affected
- Actions taken
- Evidence collected

CTF PREVIEW AND TOOL SUMMARY

Key Tools Covered:

- Nmap: Network discovery and service detection
- Text editors & grep: Configuration analysis
- Log analysis tools: Pattern recognition in logs
- File analysis: Malware identification

TEMPLATES

SahurCTF

- https://btctf.cyber673.com
- Register
- Defend (or try to)!
- Winner gets… something!

cyber673