

Countermeasures



Dale Meredith

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

dalemeredith.com | [Twitter: @dalemeredith](https://twitter.com/dalemeredith) | [Linkedin: dalemeredith](https://www.linkedin.com/in/dalemeredith)

The best protection anyone can have is
knowledge.

Dale Meredith

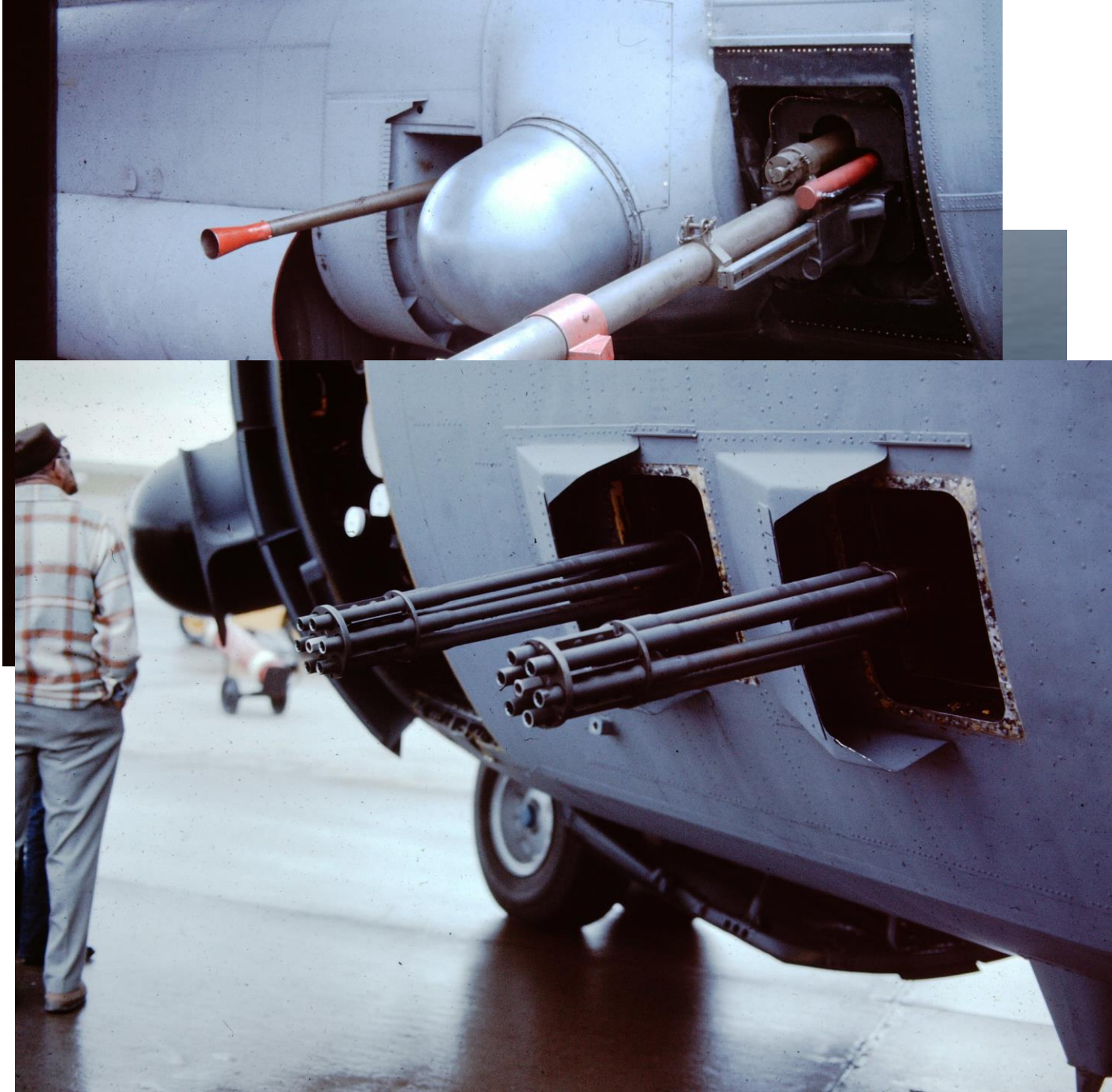


<https://t.me/learningnets>



Preventing malware from entering a system is far easier than trying to eliminate it from an infected system.

Puff the Magic Dragon



10 howitzer rounds per/min

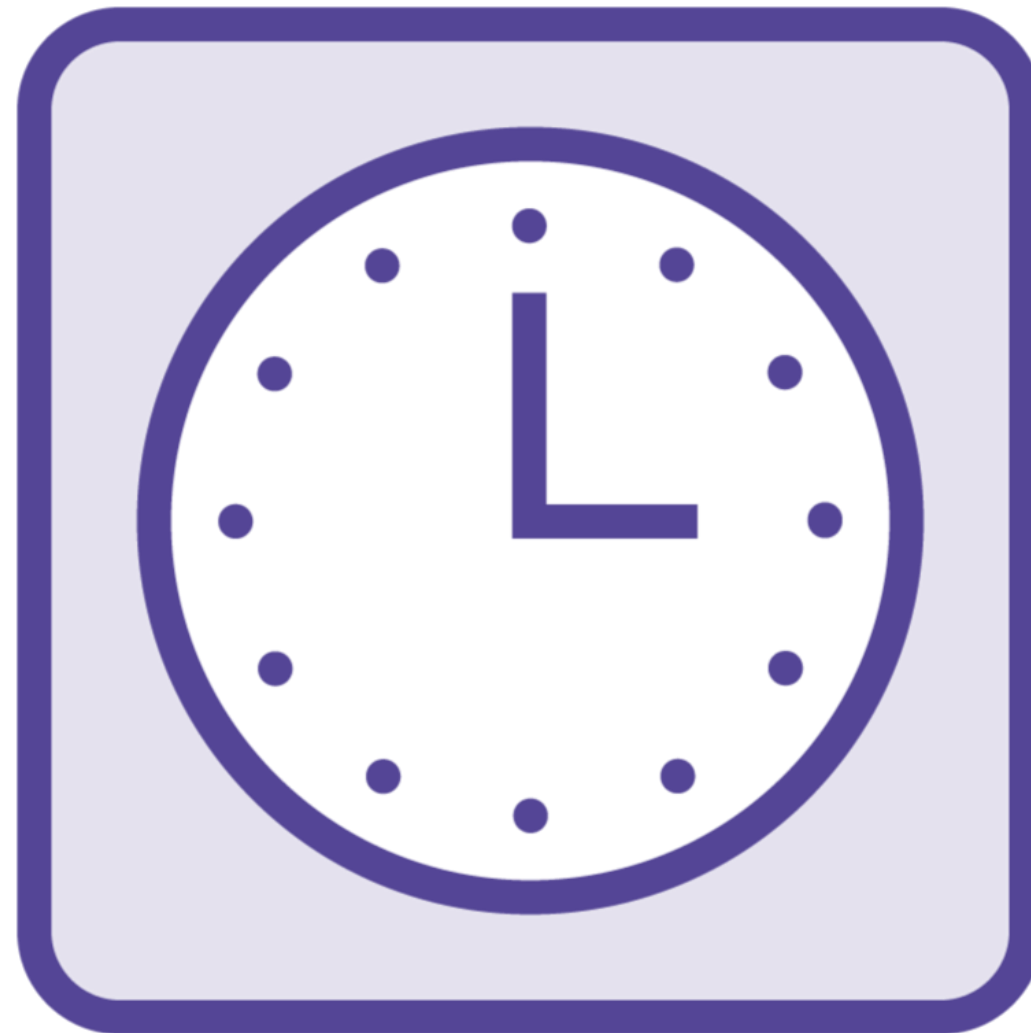
7500 rounds per/min

High value target in the battlefield

Virus Discovery Methods

Methods of Discovery

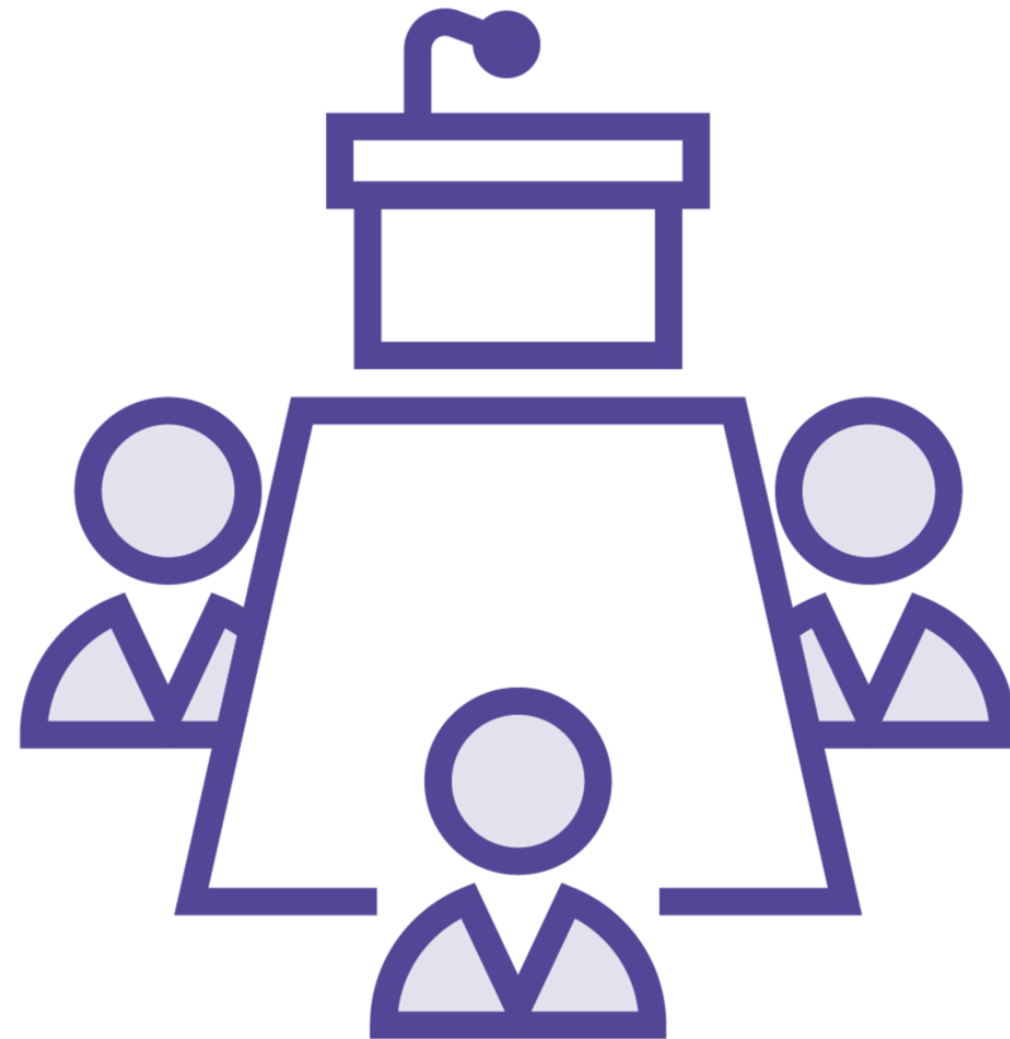
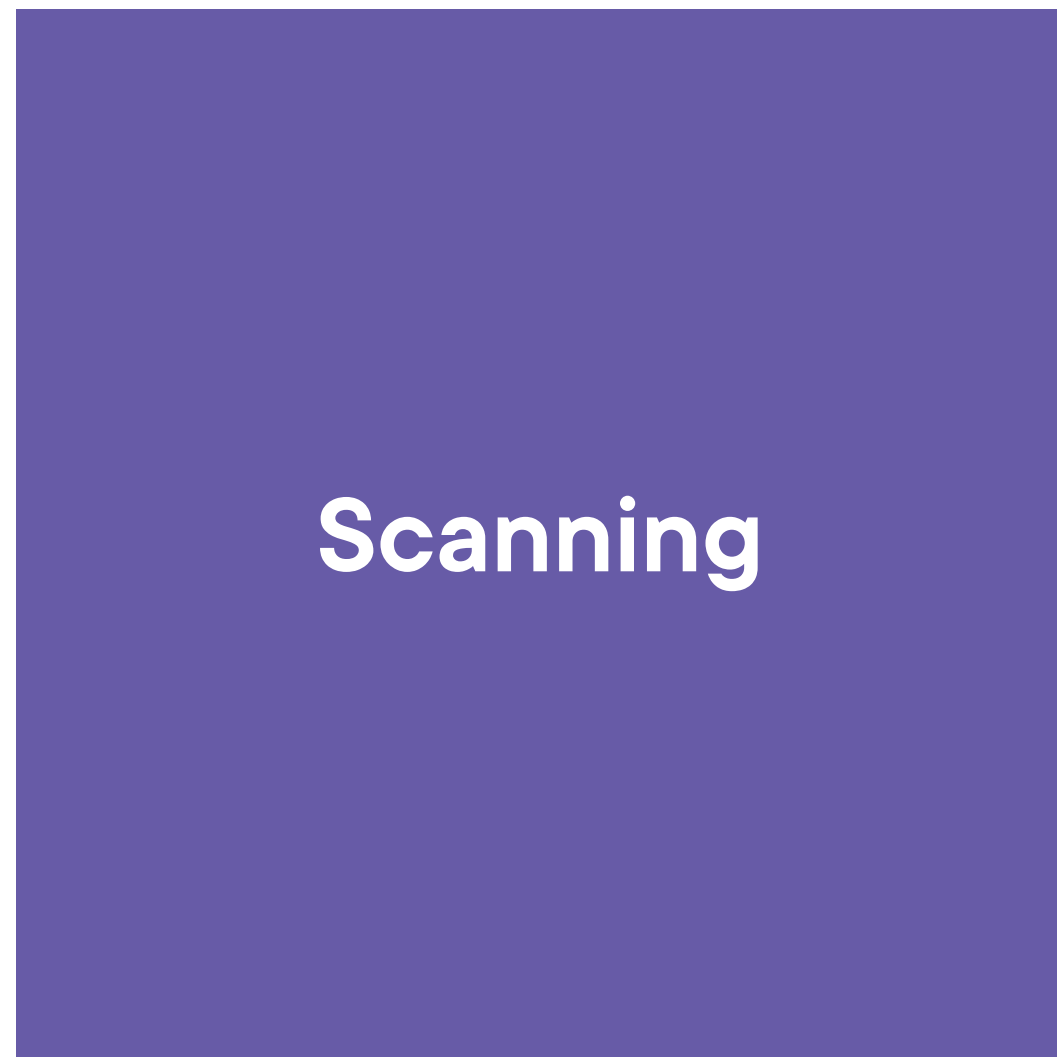
Scanning



The best is **always**
changing

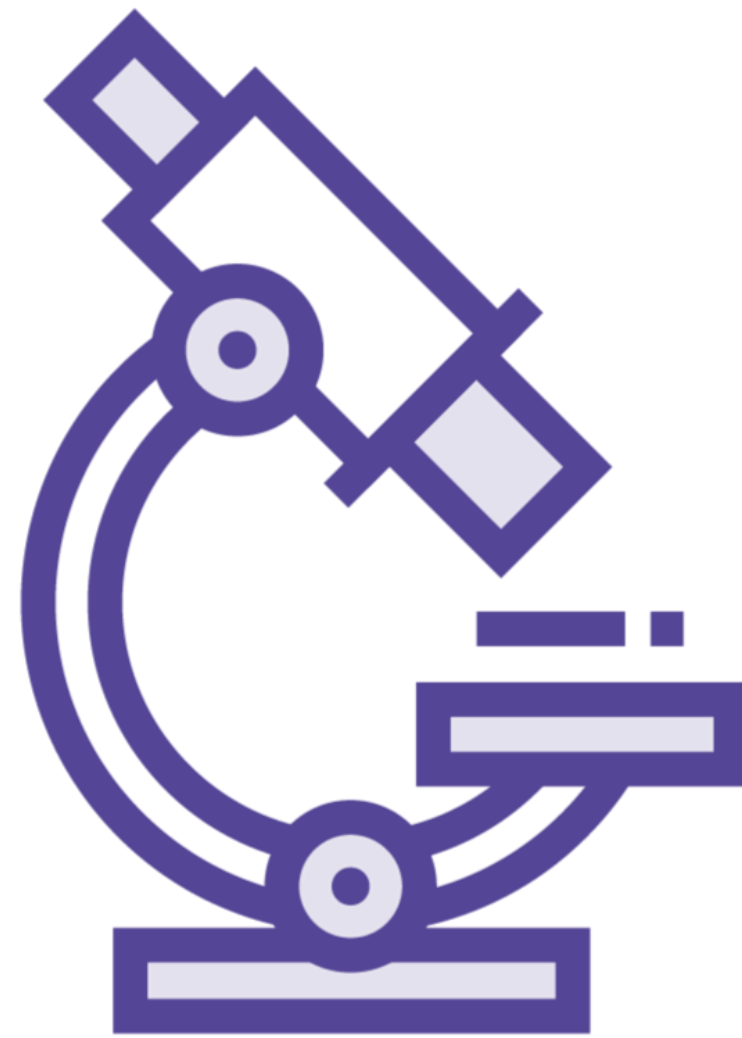


Methods of Discovery

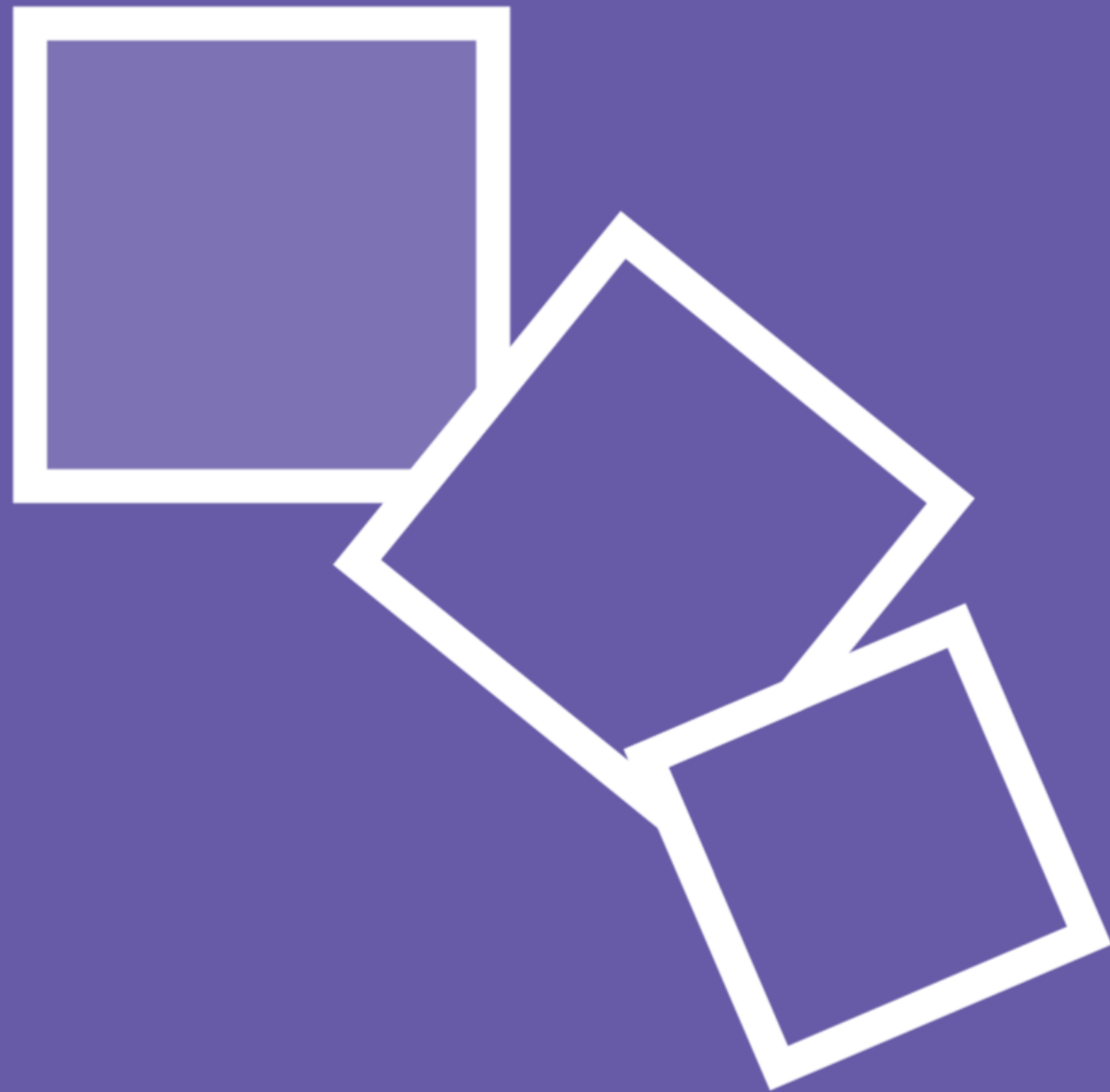


If it looks suspicious, then
consider it suspicious.

Methods of Discovery



Signature String



Methods of Discovery

Scanning

Integrity checking

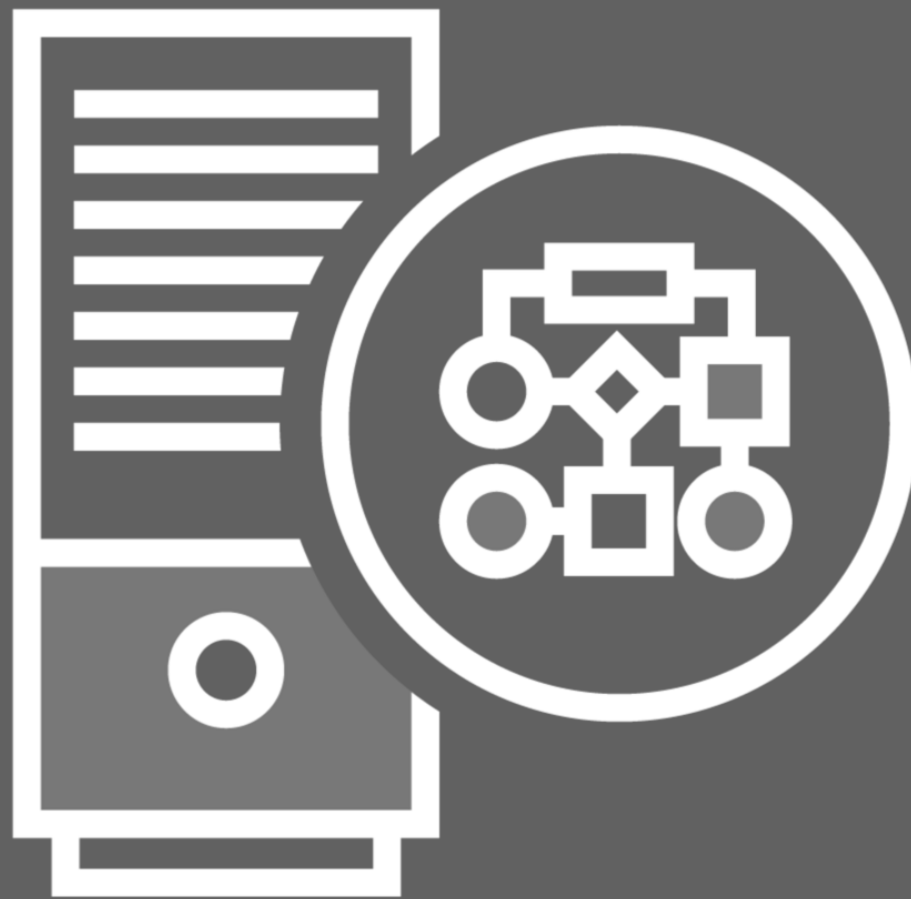
Interception



Master List

Best Practices

Three Levels



Next group of slides is another option- from the
PDF

Malware Countermeasures



**Macros and automatic
plugin downloads**



**PowerShell and WMI when
not in use**



**PDF readers to run
JavaScript automatically**



**Flash in the browser
settings**



**Unused or unnecessary
applications**

Disable

Malware Countermeasures



Two-factor authentication



Multi-layer security to detect and defend



Administrative tools and restrict access



Admin rights and provide privileges based on user level



Unused or unnecessary applications

Implement

Remove

Malware Countermeasures



User Behavior Analytics (UBA) to detect threats



Application control to prevent browsers from spawning script interpreters



Next-generation antivirus (NGAV) software



A baseline and search for known tactics

Use

Malware Countermeasures



All running programs



Indicators of compromise



Changes in the system's usual behavior pattern



Managed Detection and Response (MDR) services



Use key tools

Examine

Ensure

Malware Countermeasures



Whitelisting solutions



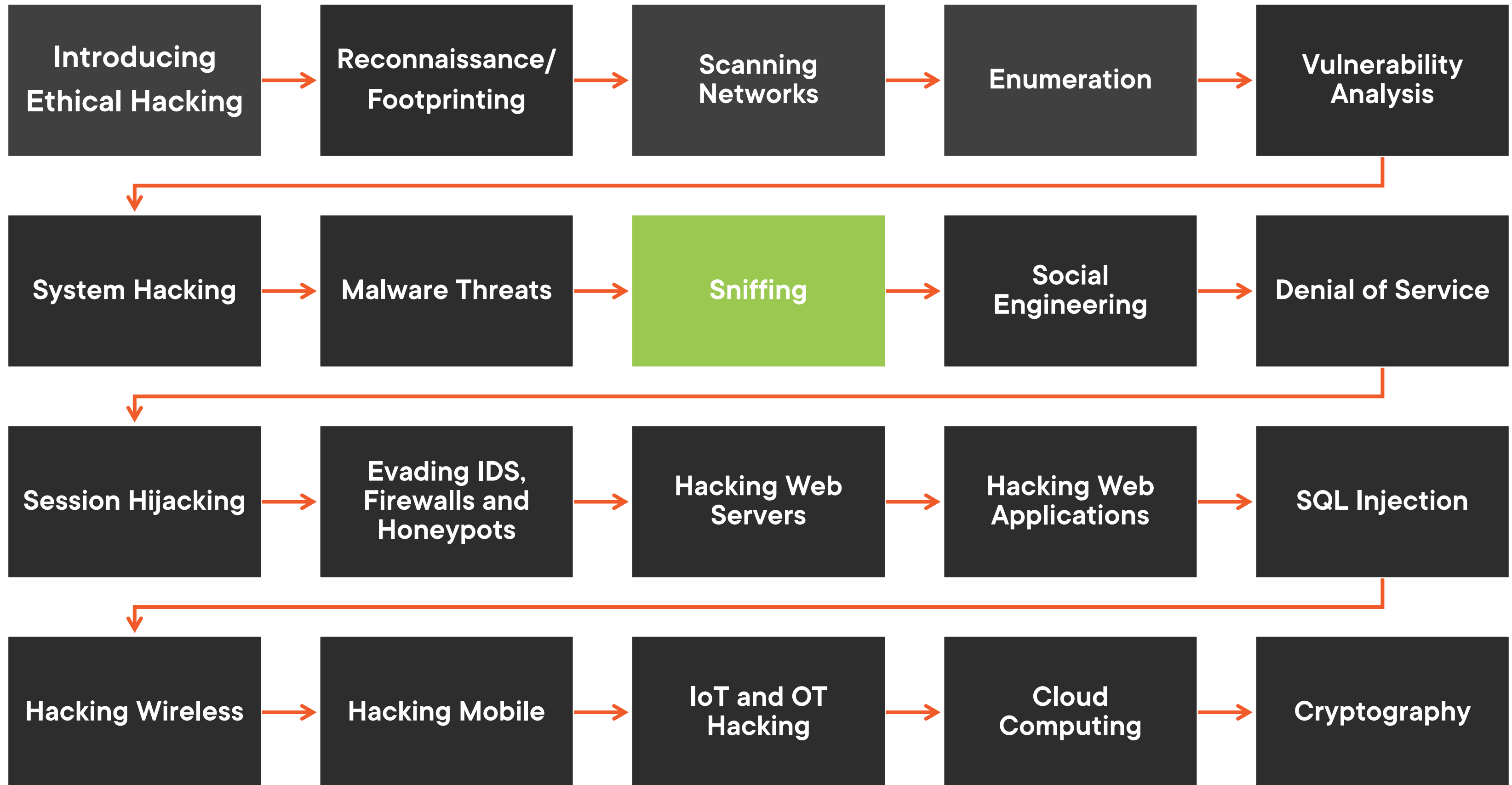
Browser protection tools

Install



Train employees

Ethical Hacking Series



Learning Check

Learning Check



Signature strings



Code analysis



Train employees



Uninstall unused apps



Watch your downloads/sources



Up Next:
Ethical Hacking: Sniffing
