Technical Weakness Identification with Nikto

Lee Allen
PENETRATION TESTER

Nikto

Nikto

Creators:
Chris Sullo and David Lodge

Nikto is a free and open source web server and web application assessment tool. The primary function of Nikto is to identify security weaknesses such as default files, misconfigurations, or published security vulnerabilities.

Nikto

GNU General Public License (GPL)

Nikto Copyrighted by CIRT, Inc.

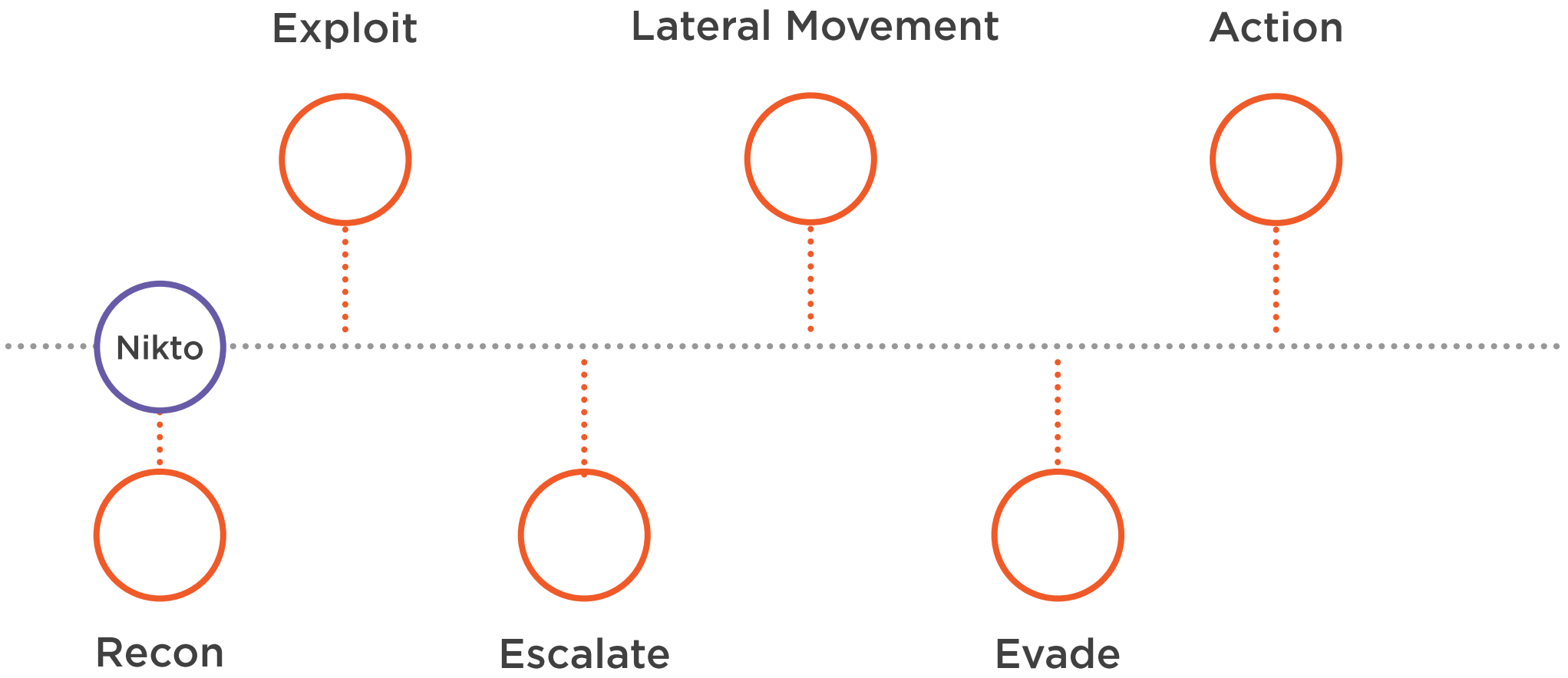
LibWhisker Copyrighted by Jeff Forristal (wiretrip.net)

Performs web server vulnerability identification

- Identifies outdated components
- Allows for replay of findings
- Identifies server and software misconfigurations
- Finds default or insecure files

Full proxy support

Kill Chain


Exploit
Lateral Movement
Action
Nikto
Recon
Escalate
Evade

MITRE PRE-ATT&CK

Tactics	Technical Information Gathering People Information Gathering Organizational Information Gathering Technical Weakness Identification People Weakness Identification Organization Weakness Identification Adversary Opsec Establish and Maintain Infrastructure Persona Development Build Capabilities Test Capabilities Stage Capabilities

MITRE PRE-ATT&CK

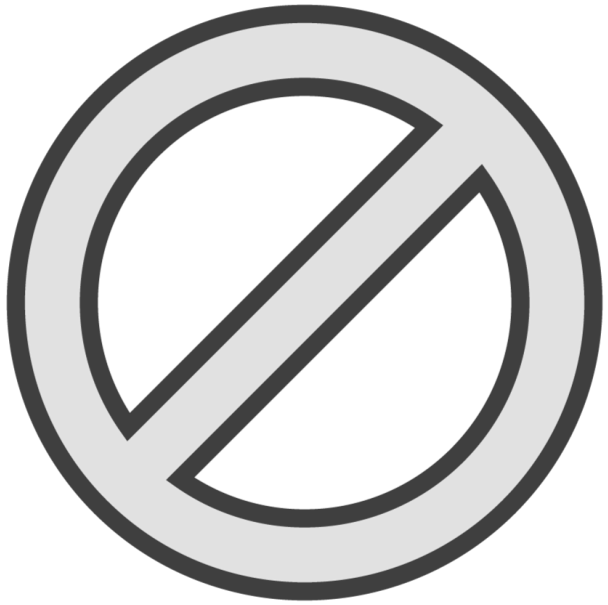
Tactics

- Technical Information Gathering
- People Information Gathering
- Organizational Information Gathering
- **Technical Weakness Identification**
- People Weakness Identification
- Organization Weakness Identification
- Adversary Opsec
- Establish and Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

T1293:
Analyze application security posture

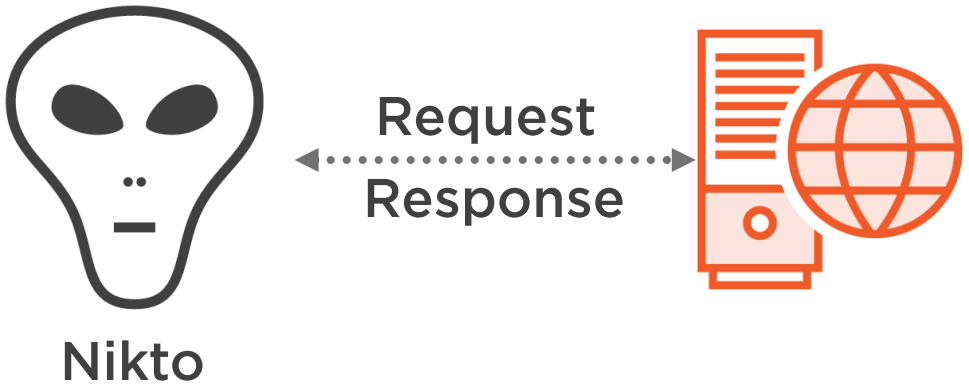
T1288:
Analyze architecture and configuration posture

Scanning Web Servers



Only test with proper permissions!

Scanning Web Servers



Misconfigurations

Outdated components

Outdated server Versions

Dangerous files

Demo

- Review Nikto command line options
- Perform a basic scan using Nikto
- Perform a basic scan against multiple hosts using Nikto
- Review available plugins
- Configure and use a Nikto plugin

Demo

Replay a saved Nikto request

Configure Nikto to use a proxy

Configure Nikto to use authentication

Create different output formats

Customize the HTML output template

More Information

Capabilities

Nikto Documentation

https://cirt.net/nikto2-docs/

Integrations

- Metasploit
- Nmap
- Nessus
- OpenVAS

Additional Resources

MITRE PRE-ATT&CK

https://attack.mitre.org/resources/pre-introduction/