Penetration Test Playbook

Recon

Passive Reconnaissance

Active Reconnaissance

Scanning and Enumeration

Run tools:

1. `nmap`
    1. Search `msfconsole` for all discovered technologies
    2. Search the web for exploits for each discovered technology
2. `autorecon.sh` in `\Tools`
3.

Initial Foothold (Exploitation)

General Information

Common Initial Foothold

> Most initial footholds are gained by malicious email attachments or exploits against the user's browser.

Example workflow:

1. See if domain is Spoofable using Spoofy
2. Create malicious macro'd excel sheet using the Nishang framework
3. Email excel sheet; use MSFconsole as C2 server(see Spear Phishing Techniques section)

Be intentional with the script you choose to embed in the excel spreadsheet. It doesn't have to be complicated, and you don't necessarily need the MSFconsole, you can embed a `DownloadString` (see PowerShell Evasion) call and use `netcat` as your listener.

> Resource: https://azeria-labs.com/initial-compromise/

Web Applications

Initial Brute Forcing

Run tools:

1. Subdomain Enumeration: `gobuster dns` or `amass intel`
2. Directory Busting: `gobuster dir` the top level domain (TLD)

    1. then, directory bust all found subdomains
3. Brute Force Login Pages: `hydra`

Persistence

Command and Control

Asset Discovery

Lateral Movement

Privilege Escalation

Resources

- Azeria Labs: APTs https://azeria-labs.com/advanced-persistent-threat/
-