Tags:
Specs:

Pre-phase: Sanity check (Optional, or if nmap fails)
IP Address ping

> Use -Pn inside AD environment

# Phase 1 - Nmap enumeration

Identifying attack vectors
Nmap command
Nmap results

# Phase 2 - Port/service enumeration

ftp/ssh/web/netbios/smb/rdp/winrm,etc. Enumerate comprehensively

# Phase 3 - Exploit

CVE/creds

# Phase 4 - Initial Foothold

Find local.txt

# Phase 5 - Target enumeration

Winpeas/Linpeas

# Phase 6 - Target exploit

CVE/misconfiguration

# Phase 7 - Root

Find root.txt

Methodology notes:

Take Away Concepts:

> Unicode
> If box is done : ✓
> If box is not done: ✖ ⃠
> Windows:
> Linux: