Ethical Hacking CS378

Group 6: Xinyi Wang, Joel Henning, Tipparat Umrod, Jeffrey Li

Network Assessment Methodology

- Network discovery*
- Host discovery*
- Service discovery*
- Host enumeration*
- Service enumeration*
- Network topology mapping*
- Vulnerability testing*
- Reporting*
- Remediation

* steps our tool covers

Goal:

- Automate a subset of network footprinting
- Facilitate analysis & assessment

3 Step Process

Step 1:

Comprehensive Nmap scan

Step 2:

SNMP

Finger

Step 3:

User Enumeration

1. Nmap Scan

Comprehensive Nmap scan: scan range of most common ports for each box

- ➔ **OS details**
  OS CPE (Common Platform Enumeration), OS details, Router info
- ➔ **Vulnerable Services**
  Open/Closed ports, finger, ssh
- ➔ **Exportable Formats**
  - Text to PDF
  - CSV to Bootstrap table

Nmap headers

- Hostname
- Ports/services
- MAC address
- Device type
- Running
- OS CPE
- OS details
- Network Distance

2. SNMP

Perform snmpwalk on the router detected from nmap scan

➔ **Guessing with Default Community String**
- public

➔ **Brute Force Community String**
- default using John's password.lst

- users can specifiy password file

3. Finger

Perform finger on every IP that has a live 79 port:

- ➔ **See if a User is logged in**
  Finger will return the any users who are logged into the box being scanned
- ➔ **Usernames collected**
  Used to try and access the boxes

4. User Enum

The usernames gotten from finger are then used to try and brute force ssh:

- **Hydra to brute force**
  Brute force each live ssh port with the usernames gathered from finger
- **Upon success reports username/password combination**
  Successful cracks allow access to the box to install malicious software or steal files

Limitations

- Lack of UI
- Easy to detect
- Brute force

Meet Marcos.

He’s a security professional.

He might just be a script kiddie, but he’s a real ethical hacker at heart, and he loves our tool for obvious practical purposes.

“This tool has everything I’ve ever wanted” - Marcos