SIGPwny

FA2024 Week 03 • 2024-09-17

Network Security & Active Recon

Ronan Boyarski

Table of Contents

Network Security Overview

Network Security Overview

- Generally, we're concerned about the security of **services**
  - A service is a piece of software that's doing something important and remotely accessible on a target computer, like remote logins, file sharing, etc.
  - Examples include default system ones (like SMB) as well as user-configured ones (FTP, web, etc)
  - Going to have different **protocols** on different **default ports**
  - The type of service is going to have a huge impact on the kinds of things we can do with it
  - Some services have features that are bad for security (e.g. Redis)

Network Security Overview

- How can we tell what a computer is running?
  - Port scanning
  - Service scanning
  - Interacting with target services
- How can we get in?
  - Known vulnerable versions
  - Misconfigurations
  - Brute force

General Attack Flow

- Before this phase, there's typically an OSINT phase of finding things like relevant IPs to attack and a number of other things, but I'll ignore that for this context
- The goal is to create an accurate model of what is going on on the target
- The flow is going to be scanning ports, identifying services, and then looking for vulnerabilities & misconfigurations
- Typically, we will start with **nmap** and use subsequent tools, sometimes in an automated fashion
- If you're having trouble gaining access, ensure that you've actually looked for as many ways in as possible

Active Recon

Port Scanning

- Port range: 0-65535, TCP & UDP
- `sudo nmap -Pn -F -sV -vv $IP -oN fast.txt`
- `sudo nmap -Pn -A -sV -p- -vv $IP -oN full.txt`
- `-Pn` skips the ping check
- `-A` means that nmap will run scripts and OS fingerprinting
- `-sV` will have the scan perform version checking
- `-p-` will scan every single port from 1-65535
- `-vv` will enable very verbose output
- `-oN` saves the result to a text file so you don't re-scan

Port Scanning - Edge Cases

- Don't forget UDP services like SNMP!
- `sudo nmap -Pn -F -sU -vv $IP -oN udp.txt`
- `-sU` will have the scan check UDP ports
- `-F` will scan top 1000 ports (UDP scanning is **SLOW**)
- If you're scanning through a SOCKS proxy, you can only scan TCP ports, and should use the **`-sT`** flag
  - This does a TCP scan rather than SYN scan
- If you're in a network, do a very fast scan using IP range
- General workflow tip: make a directory for each target

Port Scanning Alternative - Rustscan

- Rustscan is a modern, insanely fast alternative to **nmap**
- Can scan all 65535 TCP ports in **as fast as 3 seconds**
- Honestly not sure about the stealth implications of this, but obviously blazing through 65535 ports in a few seconds is highly unusual
- Great for situations where the only thing that matters is speed
- Integrates with nmap for service scanning and script execution

Service Scanning: SMB

- Server Message Block runs by default on all Windows computers (but can be disabled manually)
- If you know the password, you can view remote file shares
- If the target is running Windows Server or is AD joined, and you have Administrator credentials, **remote code execution is a feature**
- Windows computers prior to Windows 7 SP 6.1 are vulnerable to MS17-010 (SYSTEM RCE)
- Depending on the target configuration, you can potentially read/write files

Service Scanning: Other services

- FTP: can be used to upload files or download sensitive files if left unsecured
  - This is especially potent if chained with a web server w/LFI vuln
- SSH: if you have a password or id_rsa, get a shell as a feature
- Telnet: like SSH, but without the secure part (yikes)
- SNMP: Simple Network Management Protocol, allows viewing all of the running processes, usernames, and software versions, including command-line arguments
- SMTP: Simple Mail Transfer Protocol, you can send phishing emails from the command line (will cover this on 12/3)
- Redis: Database, can **gain RCE as a feature**

Service Scanning

- This is just the tip of the iceberg
- Get in the flow of understanding unfamiliar services quickly and think in terms of primitives, similar to pwn
- https://book.hacktricks.xyz/ has some good preliminary steps for interacting with and attacking unfamiliar network services
- Other really important services (like web servers & active directory) will be covered individually

Gaining Access

Gaining Access: Exploitation

- Sometimes, when attacking vulnerable software, it's as easy as running searchsploit or the relevant metasploit module
- Other times, custom exploit development is necessary
  - This is where time spend doing traditional CTF is helpful
- Example workflow:
  - nmap -> port 80 is open -> feroxbuster -> find gitlab instance
  - searchsploit gitlab
  - run exploit, hopefully get shell
- **ALWAYS** read exploit code before running it!

Gaining Access: Misconfiguration

- Sometimes, services are set up with really stupid permissions
- For example, an file server that lets you write to anything in a web server or a user's home directory would be a huge problem
- Example Workflow:
  - nmap -> port 21 & 80 -> unauthenticated FTP server with access to /var/www/html -> put webshell -> browse to port 80 -> get shell
- There are way too many possible misconfigurations to cover here
- Get in the habit of thinking about what access is appropriate

Gaining Access: Password Attack

- Lots of common software, like WordPress, doesn't rate-limit authentication, so you can go through an obscene amount of login attempts
- Hydra is a fantastic general-purpose password attack tool
- Example workflow:
  - nmap -> port 443 -> feroxbuster -> /wp-admin
  - `hydra -l Admin -P /usr/share/wordlists/rockyou.txt 10.10.230.209 http-post-form "/wp-login.php:log=^USER^&pwd=^PWD^:The password you entered for the username" -t 30`
- Use admin login to upload PHP reverse shell (feature)
- Hydra can be used to attack many other services as well

Live Example

Next Meetings

2024-09-19 • **This Thursday**

- Wireshark & Network Forensics w/Sagnik & Michael
- Learn how to detect what we did here today!

2024-09-24 • **Next Tuesday**

- Web Hacking for Red Teams
- Complement your SIGPwny web knowledge with more advanced techniques

2024-09-26 • **Next Thursday**

- Running & Containerizing Web Services with Docker