Hackoween Workshop

Shells and Privilege Escalation

Shells

Terminology:

- Terminal - the UI wrapper to run commands
- Command line - the method of interacting with the UI
- Shell - the software that interprets commands and runs them on the OS

Actual use - “pop a shell”, “spawn a shell” just allows you to run system commands

1. Web Shell
2. Bind Shell
3. Reverse Shell

Web Shell

- A webpage or endpoint that allows an attacker to run arbitrary commands on the server
- Note - this is not an RCE vulnerability, but rather a completely separate (typically attacker-created) endpoint or webpage made specifically for the attacker to run commands
  - Is often created after an RCE or file upload vulnerability is found
- Works very simply - takes in a GET or POST parameter, executes it, and prints out the result
- Can find them all over the internet, but anything not custom is practically always caught by AV

Bind Shell

- A process is started on the host where a shell (like bash or zsh) is bound to a specific TCP port. Whoever connects to the port can run whatever commands they want
- Typically on a high, uncommon port to evade detection
- Simple netcat bind shell:

  -
    ```
    nc -lvp 60234 -e /bin/bash
    ```
- Simple netcat client:

  -
    ```
    nc 10.1.1.1 60234
    ```
- After connecting, you just type commands and get the output

Reverse Shell

- When the vulnerable machine is on an internal subnet, it may be impossible for an attacker who does not have internal access to connect directly to the machine
- Firewall rules also will catch sketchy connections coming IN to random ports
- To evade this, the shell is designed to reach OUT to the attacker on it’s own, typically on a common port like 80 or 443 to evade detection by appearing like normal traffic
- The attacker must have a publicly-available TCP port to receive the connection
- No listening port on the target makes it easier to evade detection also

Basic Privilege Escalation

- Regular user → root/administrator
- Abuse extra permissions given to regular/guest users
- Exploit kernel or software vulnerabilities
- Checking files for administrator credentials, API keys, or other sensitive information
- Exploiting regularly-run scripts or software
- Exploiting incomplete or unquoted paths
- Log files
- Various tools will do a lot of this enumeration for you, such as LinPEAS or WinPEAS

Linux Privilege Escalation

- Abusing sudo permissions to spawn a shell (sudo -l)
- Writing to cronjob scripts
- Writing to other files that a user will run as sudo
- Binaries with SUID-bit set
- SSH keys
- Writable service files

Windows Privilege Escalation

- Abusing SEImpersonate privileges
- PowerShell history
- Exploiting unencrypted WSUS servers
- Unquoted paths
- Enabled default/service accounts
- DLL hijacking
- Application credentials

Competition Details

Competitions

- King of the Hill Competition (left side)
  - Teams of 2 (preferably upperclassmen & lowerclassmen)
  - Private match in TryHackMe
  - One vulnerable box, each team wants to hack in to get points, and keep other teams from getting in
- OSINT Competition (right side)
  - Teams of 3
  - Your goal will be to OSINT a target, develop a pretext, and send me a phishing email by 8:30pm
  - Purpose is to convince that person to click on a link they’re not supposed to
  - Target will be released at 7:30
- Cannot do both, must choose
- OverTheWire labs available on machines on the left

King of the Hill

- Must have a THM account (free) with skill level set to intermediate or higher
- Go to https://tryhackme.com/games/koth
- We will release a private invite code in Slack
- There is a single machine that each time wants to hack
- Get points from putting your name in /root/flag.txt, or capturing other flags hidden around the system
- Cannot shut down services or delete important files
- Uses OpenVPN to connect to the local network
- 1 computer per team (don’t believe multiple computers can use the same VPN configuration)

OSINT Competition

- Doesn’t matter what the originating email is
- Include To, From, and Subject headers **inside the body of the email**. It will be sent to justink.applegate@gmail.com, but the To header in the body of the email will be set to the target email in question
- The “malicious” link you want the target to click is https://malicious.com/.
- Allowed to OSINT the person and the organization to see what pertinent information you can find
- NOT IN SCOPE
  - OSINTing coworkers beyond names and titles, performing Nmap/subdomain scans, any web/network exploitation, etc. - there is no actual PENTESTING in this competition, just RECON
- Common ideas - pretend to be IT, their bank, close friend, etc.

OSINT Competition (continued)

- The From header should be set to a convincing email - note that the domain MUST BE AVAILABLE FOR SALE, or the username should be available
    - For example, king@gmail.com is NOT valid because that username is not available
    - king@iamthebestosinterever.xyz IS valid because the domain is available for sale
    - I will be checking this - invalid domains will be docked points.
- Email must be sent by 8:30pm ON THE DOT, winners will be announced 10-15 minutes after