CodePath

Week 6

Codepath Homework

Lab report 10/14 @ 11:59 PM

- Submitted on **Collab**
- This includes **Security Shepherd**
    - User Authentication (0 - 3)
    - Password Hashing (0 - 3)

Topics

Week 6

Readings on course website

Mostly review for attacks

- User Authentication
- Username Enumeration
- Credential Theft
- Privilege Escalation
- Brute Force Attack (review)
- Dictionary Attack (review)

User Authentication

- Recall topics such as
  - Password hashes
  - Salts
  - Multi-factor authentication
  - Key space for brute-force
  - etc

User Enumeration

- **User Enumeration:** Process of enumerating all possible usernames in an application, server, etc.
- **Strategy**: Enter random usernames to see what error-handling message you get
- **Dumpable Username Enumeration**: Manipulation that allows a full/partial list of valid users
  - Often a result of SQL Injections (as you hopefully saw)

Login Page

Username: “john”

“User john is not found”

Login Page

Username: “john”

~~“User john is not found”~~

“User not found/invalid”

Credential Theft

- **Credential Theft:** Action of retrieving a user's login credentials

- Three techniques
  - Phishing
  - Key-logging
  - Database theft

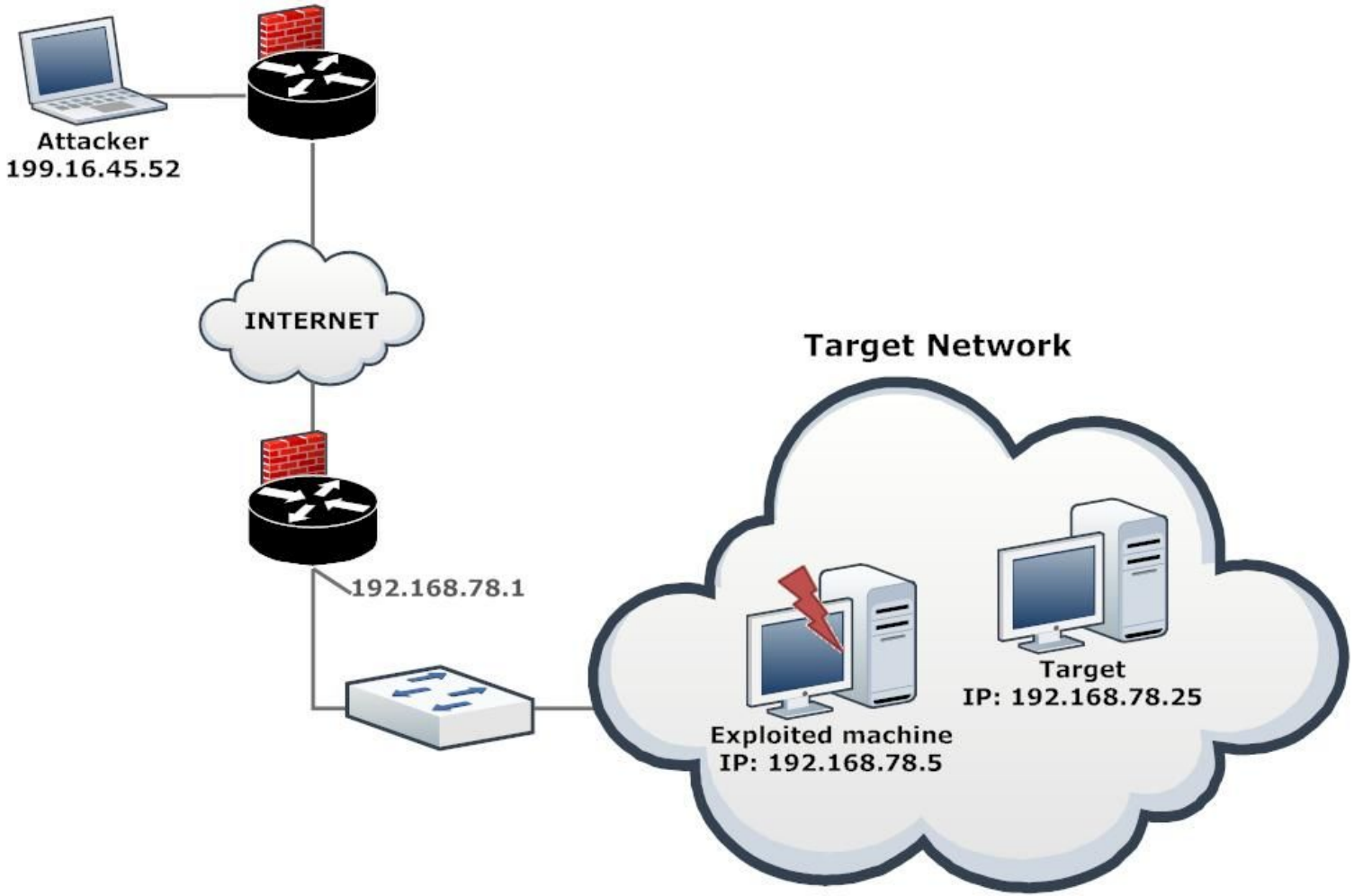
- Usually part of other attacks as well
  - IDOR
  - SQLi

Privilege Escalation

- **Privilege Escalation:** Exploiting a vulnerability such that it allows an attacker to gain access to resources which are normally restricted

- **Strategy:** Gain access to root or admin
  - Go from normal user to a root user
  - Can result due to **pivoting**
    - Using a ‘plant’ or ‘foothold’ to move around inside a network

- **Why:** For attackers to get around the “Principle of Least Privilege”


Attacker
199.16.45.52
INTERNET
Target Network
192.168.78.1
Exploited machine
IP: 192.168.78.5
Target
IP: 192.168.78.25

Recap

Which of the following should result from an incorrect username and/or password?

a) Invalid username and incorrect password
b) Invalid user
c) Invalid username and/or password
d) Incorrect password

Lab Report

- Need to do all required Security Shepherd challenges
  - You can find them under the “Lab” tab on the course page
- You need to include step-by-step instructions with screenshots on how you did them
  - Similar to extra credit for CTF’s

Lab Report

- Additionally, you need to make a walkthrough on how you got Hashcat installed/working on your machine
  - Include screenshots
- Make sure to submit a PDF in the format as described in the write-up

Hashcat

- **Hashcat:** “world’s most fastest and most advanced password recovery utility…”
- You will need this tool for the lab report
- Check these out
  - https://github.com/hashcat/hashcat
  - https://hashcat.net/hashcat/

```
hashcat (v4.2.0) starting...

OpenCL Platform #1: NVIDIA Corporation
======================================
* Device #1: GeForce GTX 1080, 2028/8112 MB allocatable, 20MCU
* Device #2: GeForce GTX 1080, 2029/8119 MB allocatable, 20MCU
* Device #3: GeForce GTX 1080, 2029/8119 MB allocatable, 20MCU
* Device #4: GeForce GTX 1080, 2029/8119 MB allocatable, 20MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
* Slow-Hash-SIMD-LOOP

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Watchdog: Temperature abort trigger set to 90c

$fvde$1$16$22626023383178883815724143841523$20000$c...05210b:hashcat

Session..........: hashcat
Status...........: Cracked
Hash.Type........: FileVault 2
Hash.Target......: $fvde$1$16$22626023383178883815724143841523$20000$c...05210b
Time.Started.....: Thu Aug  2 11:01:42 2018 (5 mins, 35 secs)
Time.Estimated...: Thu Aug  2 11:07:17 2018 (0 secs)
Guess.Mask.......: ?l?l?l?l?l?lt [7]
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:    63480 H/s (82.28ms) @ Accel:128 Loops:64 Thr:640 Vec:1
Speed.Dev.#2.....:    63446 H/s (82.85ms) @ Accel:128 Loops:64 Thr:640 Vec:1
Speed.Dev.#3.....:    64012 H/s (81.63ms) @ Accel:128 Loops:64 Thr:640 Vec:1
Speed.Dev.#4.....:    63957 H/s (81.53ms) @ Accel:128 Loops:64 Thr:640 Vec:1
Speed.Dev.#*.....:   254.9 kH/s
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 83558400/308915776 (27.05%)
Rejected.........: 0/83558400 (0.00%)
Restore.Point....: 0/11881376 (0.00%)
Candidates.#1....: hariert -> hmhifet
Candidates.#2....: hsbrndt -> hjbmyct
Candidates.#3....: gunlrlt -> gcpwhkt
Candidates.#4....: gvclyct -> ginlrlt
HWMon.Dev.#1.....: Temp: 72c Fan:81% Util:100% Core:1809MHz Mem:4513MHz Bus:1
HWMon.Dev.#2.....: Temp: 74c Fan:84% Util:100% Core:1809MHz Mem:4513MHz Bus:1
HWMon.Dev.#3.....: Temp: 71c Fan:85% Util:100% Core:1822MHz Mem:4513MHz Bus:1
HWMon.Dev.#4.....: Temp: 76c Fan:83% Util:100% Core:1822MHz Mem:4513MHz Bus:1

Started: Thu Aug  2 11:01:30 2018
Stopped: Thu Aug  2 11:07:19 2018
```

Security Shepherd Tips

- To confirm admin accounts…
  - Admin, administrator, root, superuser, manager, etc.
- Inspect the element
- Use Burp
- Brute-force some user id’s

Office Hours

Monday / Thursday / Sunday : 5 - 7 PM @ Rice 226