Vulnerability Assessment and Pentesting

Abstract

- Reconnaissance
  - Nmap - Discover hosts and services on a network
- Enumeration and Exploitation
  - Web Application security vulnerabilities
- Exploitation
  - John the Ripper - Cracks hashes for various crypt algorithms
- Vulnerability Assessment; Remediation
  - Lynis - Used for vulnerability detection, penetration testing, and system hardening.
  - ClamAV - Antivirus that detects malware, trojans, and viruses.

Vulnerability Assessment

By Deepak Mirchandani

Nmap

In case it is not already installed

- **sudo apt-get install nmap**

nmap scan (1,000 most common ports)

- **nmap scanme.nmap.org**

Find Version Numbers

- **Nmap scanme.nmap.org -A | tee scanme.results &**

Finding Exploits

- Exploit DB

CVSS and CVE

- CVSS - Common Vulnerability Scoring System
  Provides methodology to sort vulnerabilities into numerical categories

- CVE - Common Vulnerabilities and Exposures
  Entries of commonly known security vulnerabilities

  Formatting of CVE entries is in the following format: CVE-YEAR-ID (Example: CVE-2017-14956)

Attack Vector - Can be used to gain access to a service
(Example: SQL Injection allows for unauthorized access to database entries)

End Result - The attacker achieves complete access of a system

CVSS and CVE

- CVSS - Common Vulnerability Scoring System
  Provides methodology to sort vulnerabilities into numerical categories

- CVE - Common Vulnerabilities and Exposures
  Entries of commonly known security vulnerabilities

  Formatting of CVE entries is in the following format: CVE-YEAR-ID (Example: CVE-2017-14956)

Attack Vector - Can be used to gain access to a service
(Example: SQL Injection allows for unauthorized access to database entries)

End Result - The attacker achieves complete access of a system

Web App Security Vulnerabilities

[external presentation]

John the Ripper

Overview of John the Ripper

- A free and fast password cracker available for Mac, Windows, and various unix flavors.

- Download page: https://www.openwall.com/john/ (Kali-Linux has John the Ripper pre-installed)

Common use cases

- Cracks hashes such as MD5, DES, Blowfish, and other crypt password hash types.

What is a hash?

The result of using a hash function designed to protect plaintext

Examples of popular hashes:

- MD5
  Plaintext: password
  MD5 Hash: 5f4dcc3b5aa765d61d8327deb882cf99

- SHA-1
  Plaintext: password
  SHA-1 Hash:
  5BAA61E4C9B93F3F0682250B6CF8331B7EE68FD8

- DES
  Plaintext: password
  DES Hash: K.578QIvUawY2

Even changing one letter (case sensitive) in a plaintext string can result in an entirely different hash.

Exercise:

1. Open a terminal session in Kali.
2. Generate a md5 hash by executing this command:
   “ **echo -n password | md5sum** “
3. Try different combinations of a word to see the hash.

John the Ripper usage

Two basic requirements to crack hashes :

1) A wordlist
2) A password file with a hash

John has a default password list that can be used. You can locate it by executing “ **locate password.lst** “
To set a custom password list, edit the wordlist setting in the configuration file by executing
“ **john --wordlist=customlist.lst passwdfile** “

To use John the Ripper:

1) Open terminal
2) Type “john” with nothing preceding it and the intended arguments proceeding it.
   (example: **john /Desktop/hashfile.txt --show**)

Documentation:
https://www.openwall.com/john/doc/EXAMPLES.shtml

Additional Information

There are popular methods of cracking passwords in John the Ripper:

- **Wordlist mode** - Simple but slow cracking mode that uses a wordlist to crack passwords. To ensure fast runtime, sort your wordlist in alphabetical order.
- **Single crack mode** - Uses login names, user home directory names, and GECOS / Full Name fields as candidate passwords. Faster than wordlist mode.
- **Incremental (Bruteforce) mode** - Attempts all possible character combinations as passwords. Specify a password length limit to ensure the process lifespan ends in reasonable time.

To specify a cracking mode, use the following arguments (**--increment, --single, or --wordlist**)

Mangling Rules - Effective, but resource intensive method of generating similar passwords.

Example:
Base word = password
Leetify = P4ssw0rd
Append/prepending => h3r3p4ssw0rd!

To use mangling rules add the “ --rules “ argument when starting a session

Cracking System Passwords

- What is the shadow file?
  An unreadable system file where user passwords are encrypted and stored

- What is the passwd file?
  A readable system file where user details except for passwords are stored

- Using John to crack user passwords

1. Unmask the shadow file by using this command
   (“ **unshadow /etc/passwd/ /etc/shadow > hashfile** “)
2. Begin the cracking process by executing
   (“ john hashfile --show“)

Side notes:

- The shadow file cannot be read without using the unshadow command
- All cracked passwords are stored in the **john.pot** file
- **If** a shadow file does **not** exist, execute (“ **pwconv** “)

Cracking external hashes

- Cracking hashes in other files
  Instead of unmasking the shadow file, use a another file with hashes.

  Example:

  “ **john /root/Desktop/hashfile --format=raw-md5 --wordlist=password.lst --show** “

  This command attempts to crack a raw md5 hash using wordlist mode.

  Note: All cracked hashes can be located in the ***john.pot*** *file (To find execute, “* ***locate john.pot*** *“)*

Exercise:

1. Generate a MD5 hash (**echo -n password | md5sum**) and save to a file
2. Crack the MD5 hash using a wordlist

Summary

John the Ripper can be used for:

- Cracking MD5, DES, SHA, and other hash types
- Incremental (bruteforce), dictionary (wordlist), and hybrid cracking methods

Kali Linux commands:

- Nano/Cat
- Touch
- Echo
- Unshadow
- Locate

Review Challenge

1. Go to this URL: http://challenge1.litesandbox.me/index.php
2. Obtain the raw MD5 hash
3. Crack the raw MD5 hash
4. Login to the dashboard
   Use the Jumbo rule when cracking the password (**--rules=Jumbo**)

Remediation: Lynis and clamav

Lynis

- Performs an extensive heath scan on Unix machines.
- Used for three things; System hardening, auditing, and compliance testing.
- Pre-installed on Kali.
- Can perform both local and remote scans.

Lynis

Get help on lynis

- lynis

Run a lynis scan on your system

- lynis audit system

ClamAv

- Open-source antivirus software for unix machines.
- Able to detect common malicious software and viruses.
- Integrates with other software such as pfSense

ClamAv

Install

- **sudo apt-get install clamav**

More details on how to run a scan

- **man clamscan or clamscan --help**

Run a scan on your entire machine

- **clamscan**

Summary

- Reconnaissance
  - Nmap - Discover hosts and services on a network
- Enumeration and Exploitation
  - Web Application security vulnerabilities
- Exploitation
  - John the Ripper - Cracks hashes for various crypt algorithms
- Vulnerability Assessment; Remediation
  - Lynis - Used for vulnerability detection, penetration testing, and system hardening.
  - ClamAV - Antivirus that detects malware, trojans, and viruses.

Try the exercise: http://challenge1.litesandbox.me/index.php