FANSHAWE

INFO-6065

Ethical Hacking & Exploits

Information Gathering

Agenda

- Review of Lab-01
- Information Gathering Theory
- Review of Classification and Prioritization Systems
- Lab 02 Overview

Warning

- This is course is **NOT** designed to teach you how to be a hacker
- You are **NOT** allowed to use the tools and techniques we will be covering outside of the isolated lab environment
- Use of these tools on the rest of the College’s network would constitute an **Academic Offence**
- The College has full packet capture capabilities to track down illegal activity

File Integrity

We verified the checksum of our VM downloads using the MD5 hash algorithm

This ensures that the VM files we downloaded:

- Were not modified or altered in any way from the original
- Were not corrupted during download
- Are the correct files

SSH Keys

We regenerated the SSH keys on our Kali VMs

A real world example of when you would need to do this is provided by the Heartbleed vulnerability

- Archived old keys
- Created new keys
- Confirmed the two sets of keys were indeed different

SSH Keys

Note that the DSA key pair was not regenerated

- You would have two extra keys in the default directory

OpenSSH 7.0 and up disabled the ssh-dss algorithm citing its weakness as the reason

https://www.openssh.com/legacy.html

Wildcards

Wildcards are meta characters

- Characters that have special meaning to the OS
- * and ? are two very handy wildcards
- * can be used to replace in string of characters
- ? can be used to replace a single character

Wildcard Examples

mv * /etc/tmp

will move all files from the current directory to /etc/tmp

mv *.txt /etc/tmp

will move all files that end with .txt from the current directory to /etc/tmp

Wildcard Examples

```
mv ssh_host_*  /etc/tmp
```

Will move all files that start with ssh_host_ from the current directory to /etc/tmp

```
mv ssh_host_  *  /etc/tmp
```

Will try to move a file called ssh_host_ from the current directory to /etc/tmp, then will move all the files from the current directory to /etc/tmp

Wildcard Examples

mv ????.txt /etc/tmp

Will move any files who’s names are four characters long and end with .txt to /etc/tmp

mv a???.txt /etc/tmp

Will move any files who’s names are four characters long and start with an a to /etc/tmp

Information Gathering

Information Gathering

There are a wide variety of penetration testing methodologies

- I’m going to move this course more in line with OSSTM (Open Source Security Testing Methodology)
- You can get the Open Source Security Testing Methodology Manual online for free
- In most systems, information gathering usually falls into the second phase
- After you have defined the scope / objectives and attained all the necessary permissions

The goal of the information gathering phase is to collect as much information about the targets as possible

Information Gathering

You will spend the majority of your time gathering information about the targets

- 90% of the time is spent profiling the organization
- 10% of the time is spent actually launching the attack

Effective information gathering reduces the chances that your activities will be discovered

- Focusing on exploits that actually have a chance of succeeding
- Instead of spraying the network with exploits you are targeting a known vulnerability

Vectors

Vectors deal with how you are going to perform the ethical hacks

- Do you need to perform the hacks from outside the organization
- Do you need to perform the attack as though you are a guest on the internal network
- Do you need to perform the attack as an employee of a particular department on another department
- Research employee attacking HR or Finance

Channels

- For the different vectors of attack, there will be different channels that need to be considered
  - You can think of these as what system or entity you are going to interact with
- Five Channels broken into three Classes

Class	Channel	Examples
Physical Security	Human	Interacting With People
	Physical	Gaining Physical Access
Spectrum Security	Wireless	Wireless Devices
Communications Security	Telecommunications	Mostly Phones
	Data Networks	Wired Networks

INFO-6065 Focus

This course will focus mainly on hacking the Spectrum and Communications Security Classes

Wireless Devices

- Looking into the vulnerabilities of SOHO and Enterprise level wireless deployments

Telecommunication Devices

- Looking into the vulnerabilities of mobile phones

Data Networks

- The primary focus will be on the vulnerabilities of various hosts on wired networks
- Servers, End User Workstations, etc.

Information Gathering Steps

There are seven general phases you move through with gathering information

- Finding general information about the organization
- Determining network ranges
- Identifying active machines
- Discovering open ports and points of access
- Fingerprinting operating systems
- Discovering what services on running behind open ports
- Creating a detailed map of the network

Information Gathering

There are two types of information gathering:

Passive

- Uses third party services and public resources to gather information about the target
- There is a low likelihood that your activities will be discovered during with passive information gathering techniques

Active

- Defined by the fact that it introduces network traffic into the target network
- There is a greater chance that your activities will be discovered with active information gathering techniques

Passive Techniques

Passive tools we will use this week:

CeWL

- Keyword Gathering

theHarvester

- e-mail account, username, and hostname / subdomains gathering tool

whois

- Used to gather information about the entity who registered a domain

spiderfoot

- Queries public data sources

Active Techniques

Active tools we will use this week:

nmap

- Command line tool for performing host discovery, port scanning, version detection and more

UnicornScan

- Another command line scanning tool
- Similar to nmap

Other Sources of Information

Google

- This seems obvious, but you can find an incredible about of information through effective searches
- Google Hacking for Penetration Testers
- Satellite Images
- Street View
- Much, Much More

People Search Sites

- Canada411
- Yahoo.Canada411

Other Sources of Information

www.archive.org

- Non-profit that is building a Library of the Internet
- Of particular interest is the Wayback Machine
  - Searchable archive of the WWW
  - Allows you to see the original source code from previous version of a website
  - Companies often don’t start spending money on security measures until they reach a certain size
  - If you can access sites before they were being properly sanitized you can gather valuable information

Other Sources of Information

Job Sites

- Valuable resource when trying to determine a companies infrastructure
- Job postings often include a complete list of the software and hardware a new hire will need to support
- Often contain contact information for key individuals

Example of a Job Posting

- Windows 10 & Windows Server 2016
- Apache Web Server / Microsoft IIS / Tomcat
- Ubuntu / Cent OS
- Zimbra / Exchange
- MySQL / PostgreSQL
- Voxco Command Centre
- VMWare VSphere
- Perl / PHP / ASP / Java
- Avaya Aura Contact Center & CS1000
- Asterisk

Social Engineering

Over 80% of attacks are initiated through a form of social engineering

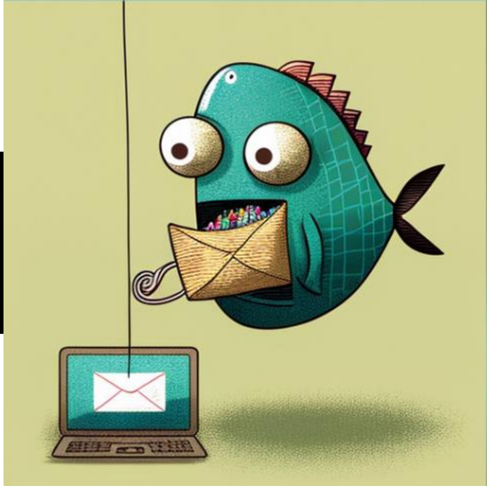
These can come in various forms

- Often present a sense of urgency
- Primary goal is to obtain unauthorized access

Involves psychological manipulation to be successful

- Easiest way to get access is to as

Phishing Attacks



Phishing techniques can come in different forms

- An email containing suspicious links
- A text message (SMS) with a link or a simple question to
- engage conversation
- A telephone call from a fraudulent source

Usually, the source is disguised as originating from a popular service or company

Attackers target an emotional/irrational response from a sense of urgency

Vishing Attacks

A new name for Telephone scams

- Target an emotional/irrational response from a sense of urgency
- Typically, the source is disguised as someone of authority (Police, government, etc.)
- Automated recordings requesting a call back to verify information, etc.

Attackers will seek to extort money

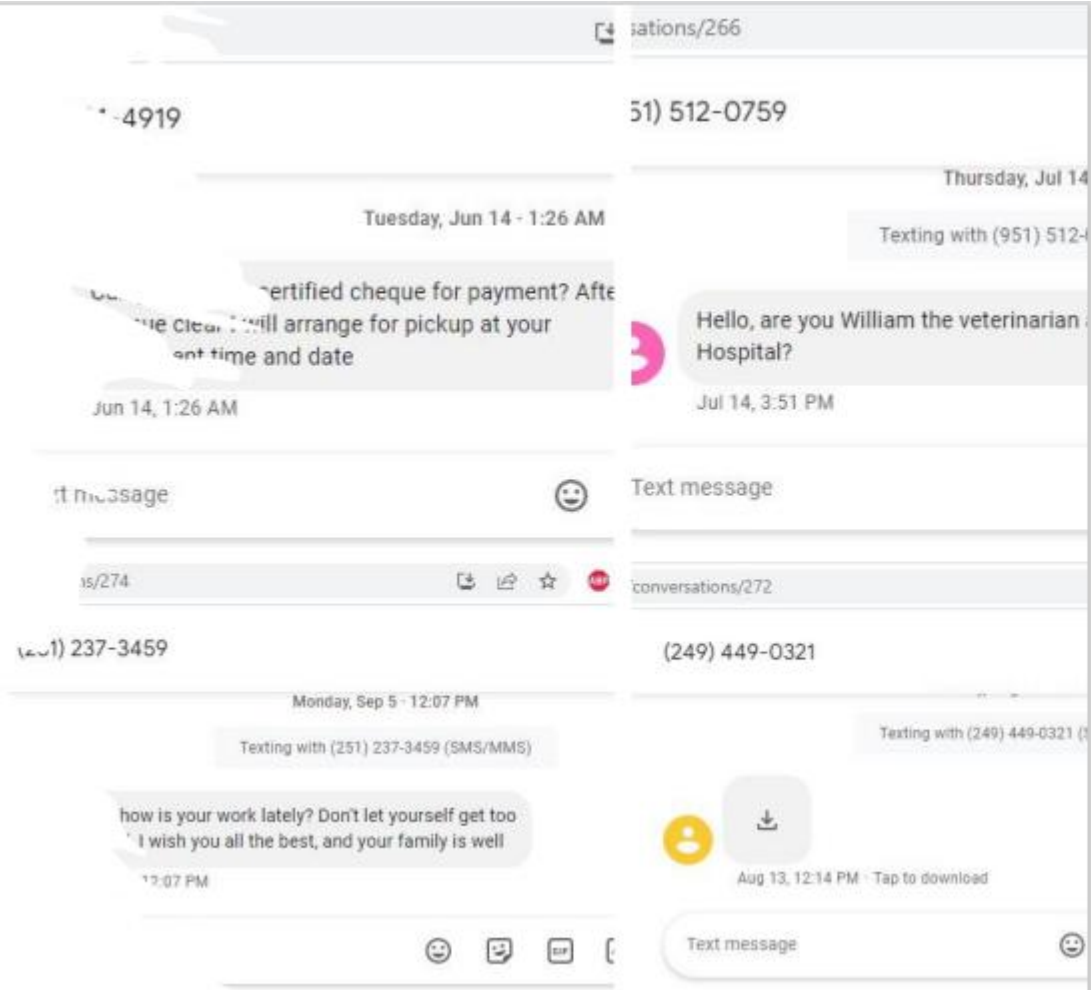
- May be in the form of gift cards
- May claim to have a relation to you

Smishing Attacks

A way to extract money or data through text messages

- A text message (SMS) with a link or a simple question to engage conversation

- Attackers will seek to extort money or gain unauthorized access



-4919

Tuesday, Jun 14 - 1:26 AM

ertified cheque for payment? Afte
e clea will arrange for pickup at your
ent time and date

Jun 14, 1:26 AM

t message

s/274

1) 237-3459

Monday, Sep 5 · 12:07 PM

Texting with (251) 237-3459 (SMS/MMS)

how is your work lately? Don't let yourself get too
I wish you all the best, and your family is well

12:07 PM

sations/266

51) 512-0759

Thursday, Jul 14

Texting with (951) 512-

Hello, are you William the veterinarian
Hospital?

Jul 14, 3:51 PM

Text message

conversations/272

(249) 449-0321

Texting with (249) 449-0321 (

Aug 13, 12:14 PM · Tap to download

Text message

Classification Review

Weaknesses

Weakness

- A generic flaw that can lead to a unique vulnerability or exposure

CWE

- Common Weakness Enumeration
- Formal list of software weaknesses
- This is a more general classification

Vulnerabilities & Exposures

Vulnerability

- A unique instance of a weakness (flaw) that can be used to access a system or network

CVE

- Common Vulnerabilities and Exposures
- Provides unique identifiers for publicly known information security vulnerabilities
- Each CVE contains
  - CVE Identifier Number
  - Brief description of the security vulnerability or exposure
  - Pertinent references

Vulnerabilities

To be considered a Vulnerability it must:

- Allow an attacker to execute a command as another user
- Allow an attacker access to data that is contrary to the specified access restrictions
- Allow an attacker to pose as another entity
- Allow an attacker to conduct a DoS attack

Exposure

An **exposure** is a configuration issue or mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network

- Doesn’t directly allow compromise, but could be an important component of an attack
- Exposures can be considered violations of a reasonable security policy
- Is a primary point of entry that an attacker may attempt to use to gain access to the system or data
- Allows attacker to conduct information gathering activities
- Allows an attacker to hide their activities

CPE

CPE: Common Platform Enumeration

- Maintained by NIST, National Institute of Standards and Technology
- Structured naming scheme for information technology systems, software and packages
- Allows researches to know they are talking about the same platform
- Based on syntax for Uniform Resource Identifiers (URI)
- Current CPE version is 2.3

CPE 2.3 Format

cpe:<cpe_version>:<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>:<sw_edition>:<target_sw>:<target_hw>:<other>

Example:

cpe:2.3:o:microsoft:windows_7:-:sp2:*:*:*:*:*:*

https://nvd.nist.gov/products/cpe

https://cpe.mitre.org/about/CPE

Older CPE Format

cpe:/part:vendor:product:version:release:edition

- Part is one of h, a, or o for hardware, application, operating system
- Vendor is generally derived from the primary domain name (microsoft.com -> microsoft)
- Product, version, release and edition are self explanatory

Previous CPE Example

cpe:/o:microsoft:windows_server_2008:r2:sp1:x64

- Vendor: microsoft
- Product: windows_server_2008
- Version: r2
- Revision: sp1
- Edition: x64

CWE, CVE, CPE

Together they allow for researchers and security professionals to know:

- What specific weakness they are talking about
- The possible vulnerabilities and exposures
- What specific platform they affect
- This becomes very important when you are trying to research an exploit to run against a specific target

CVSS

Common Vulnerability Scoring System

- Industry standard for accessing the severity of computer system security vulnerabilities
- Provides a means of prioritizing vulnerabilities

Comprised of three metrics:

Base: qualities intrinsic to the vulnerability

Temporal: characteristics that evolve over the lifetime of a vulnerability

Environment: characteristics that are dependent on the implementation / environment

CVSS

Base Metrics are further divided:

Exploitability Metrics

- Local or remote
- Complexity of attack
- Is authentication required

Impact Metrics

- Exposure of confidential data
- Damage to the integrity of the system
- Impact on availability

CVSS

Scores & Severity

- Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9
- Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9
- Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0

Having scores and scoring categories allows organizations to prioritize their responses

Lab 02 Overview

Lab 02 Overview

- Setting up targets
- Additional configuration
- Active and Passive Information Gathering

Note: make sure you do another **apt-get update** and **apt-get upgrade** the night before, or the morning of, your lab. You don't want to spend the whole lab waiting for the upgrade to finish