Lab 1: *Websites, Breaches & Games*

Lab Report Submission

Name: Van Linh Ha
Student Number: 116592171

Part 1

1. **List the top 3 general sites with an explanation of why you picked those sites and why you ranked them in that order.**
   1) Wired
      - Focuses on business security and new technology base on AI technology, automation devices and robot
   2) ZD Net
      - New technology website just released focus on business technology, education, agriculture, software and mobile security
      - They give product reviews and client can be able to download the specific security software from company website.
   3) The Register
      - Focus on business security, software and hardware part.
      - Release a newspaper article periodically

2. **List the top 3 specialized sites with an explanation of why you picked those sites and why you ranked them in that order.**
   - **Naked Security**
     - Provide antivirus software for free to client to protect endpoint devices
     - Provide wide-range of security to million clients all over the world with specific technology.
   - **The hacker News**
     - High rating newspaper platform in IT security field
       - More than 8 million subscribers from all over the world
       - Latest update technology from the Internet
       - Leading the future with new technology
   - **Threatpost**
     - Good information about business security and
     - Great company team for making the great contend as video and report about security and IT field

3. Provide a description of each of the security conferences and local groups. What is their focus? Who is their audience? What is interesting about each? Find interesting videos of some talks at these conferences. Describe them.

- DEF CON
  - Started in 1993
  - One of the largest hacker convention and attendees include:
    - Computer security professionals
    - Journalists
    - Lawyers
    - Students
    - Hackers
  - The event consists of several speakers about hacking-related subjects, as well as cyber-security challenges and competitions
- black hat
  - Security consulting, training, and briefings to hackers, corporations, and government agencies around the world.
  - People who attend these conferences are ones that are interested in information security
    - Executives and hackers
  - There are 2 parts for black hat:
    - Briefing:
      - Topics on identity and privacy, and hacking.
    - Training:
      - Training is offered by individuals working in the IT field
- SECTOR
  - Professionals gather around and learn together and interact with the world's most innovative and intellectual security specialists.
  - Sector is known for bringing in experts from all over the world to share their experiences and latest researches.
- BSides (Toronto)
  - Based in Toronto that puts together conferences on Cyber Security.
  - The purpose of Bsides is to discuss on topics beyond the IT security field. Everyone will have an opportunity to express and participate in the conference (they encourage everyone to participate). There will be all forms of interaction and they include: discussion, demos and participation.
- BSides (Las Vegas)
  - They are an organized event put together by volunteers. They stress the importance of providing free information for everyone to have access to..
  - This is a well-known global movement with a focus on increasing security awareness.
    - Main purpose is to grow the community and provide free education
  - over 300 events, in 100 cities in 26 countries on 6 continents
- Hackfest
  - largest hacking event in Canada
  - Over 900 participants
  - It is a 2 days conference followed by a 3 day training. Training will cover topics that covers hacking and security.
- CanSecWest
  - Bringing the IT community together to improve networking.
  - 3 day conference that covers presentations and are organized by professional
    - It is one hour presentations that normally begins at 9AM.

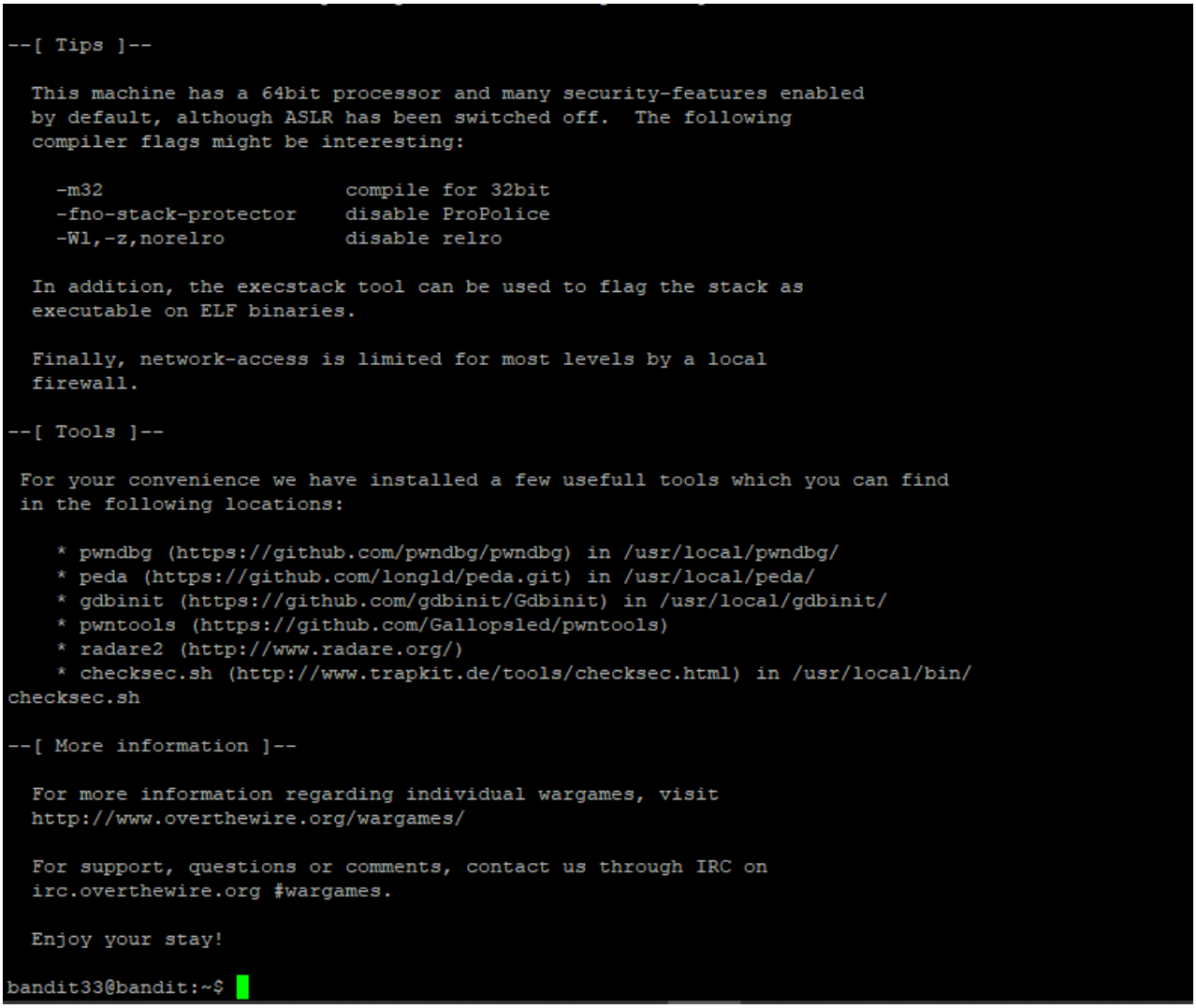
- TASK
  - It is a forum based that encourage discussion and sharing opinion on latest IT trends that may threaten computer networks.
  - Discussions are held monthly in the Greater Toronto area.
  - Discusses about:
    - New technologies that impact information security
    - Emerging threats
    - Managing security
  - Encourage discussion and share expertise in understanding the latest trends and security threats facing computer networks, systems and data.
  - Discussion is free and everyone is encourage to participate
- DEFCON416
  - It is a community for ones that have a fond interest in information security.
  - No requirements are needed; everyone from all skill levels are welcomed
  - increase the awareness of ethical hacking and develop a community that will participate in active monthly hacker events
  - Held every month
  - Topics of discussion include: web application IOT, automobile hacking.

Part 2: Breaches

The purpose of this part of the lab is to analyze some of the privacy breaches that have been in the press. Doing so will allow you to create a comprehensive picture of these breaches and their implications for the companies and their customers.

Data	**Description**
Company:	Newegg
Method:	Credit card skimming code website injection
Data Lost (volume)	50 million
Data Lost (types)	Credit card info
Company Impact	Customers left NewEgg to another retail companies
Customer Impact	Customers have to disable their bank account by themseft
Remedial Action (data loss)	NewEgg company emailed to all the customers who were potential hacked to ask them reissue their new credit card
Remedial Action (breach)	IT Department removes hacking code from their website

Part 3


--[Tips]--
This machine has a 64bit processor and many security-features enabled
by default, although ASLR has been switched off. The following
compiler flags might be interesting:
-m32 compile for 32bit
-fno-stack-protector disable ProPolice
-Wl,-z,norelro disable relro
In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.
Finally, network-access is limited for most levels by a local
firewall.
--[Tools]--
For your convenience we have installed a few usefull tools which you can find
in the following locations:
* pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
* peda (https://github.com/longld/peda.git) in /usr/local/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
* checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/
checksec.sh
--[More information]--
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/
For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.
Enjoy your stay!
bandit33@bandit:~$

REFERENCES

About us – BSides Las Vegas. (n.d.). Retrieved January 14, 2019, from https://www.bsideslv.org/about-us/

Black Hat. (n.d.). Retrieved January 14, 2019, from https://www.blackhat.com/

CanSecWest Vancouver 2019. (n.d.). Retrieved January 14, 2019, from https://cansecwest.com/

DEF CON Hacking Conference. (n.d.). Retrieved January 14, 2019, from https://www.defcon.org/html/links/dc-about.html

DEFCON Toronto. (n.d.). Retrieved from https://dc416.com/

Hackfest. (n.d.). Retrieved January 14, 2019, from https://hackfest.ca/en/about/

OWASP Toronto. (n.d.). Retrieved January 14, 2019, from https://www.owasp.org/index.php/Toronto

Sector. (n.d.). Retrieved January 14, 2019, from https://sector.ca/about/

TASK. (n.d.). Retrieved January 14, 2019, from https://task.to/