CYBER SECURITY

Team IOT

Abishek Pidwa
Alla Frefer
Anirudh Khandelwal
Prashant Bhushan
PROJECT POINTS

- Purpose
- Research Design
- Research Questions & Hypotheses
- Literature Review
- Finding & Discussions
PURPOSE

This project explores the proposed research questions using two main platforms:

- Shodan
- HackerWeb
RESEARCH DESIGN

Consists of 2 parts:
- Collection Methods
- Analytic Methods
COLLECTION METHODS

HackerWeb:
• Using SQL queries for HeidiSQL and MySQL, data was extracted from HackerWeb.
• Further analysis of posts relating to threads.

Shodan:
ANALYTIC METHODS

• Shodan Maps were used to map various devices geographically
• Hadoop used for text mining and finding text patterns
• IBM’s BigInsights and Hadoop to organize data in structured format and display in the form of graphs and pie charts
• Microsoft Excel was used in for graph creation
RESEARCH QUESTIONS

Research Question 1: What vulnerabilities are hackers taking advantage of in social networking? What techniques are being used in regards to hacking social networking sites? What incentives are encouraging hackers to do hack to social networking?

Research Question 2: What types of gambling are taking place? Which gambling are more prevalent?

Research Question 3: What online games are hacked the most? What are the incentives for hacking games?

Research Question 4: What types of attacks are being used the most? For what purposes are these attacks? Where are the source of attacks showing up the most?
RESEARCH Q1: HYPOTHESES

• By detecting keystrokes, hackers are able to figure out user’s password. We believe vulnerabilities may include security holes which allow hackers to identify these keystrokes.

• We believe the techniques being used for hacking include social engineering. For example, in Facebook tagging friends with weak privacy settings may lead to an opportunity for hacking. Other social engineering methods may include phishing emails.

• Incentives maybe financial, political, or to prove a point.
RESEARCH Q2: HYPOTHESES

• We anticipate that illegal gambling is the most prominent form.
• We think Facebook Poker will be the most popular.
• We think people are sharing high level C++/C codes to run the scripts on the different games and win the game.

• We think that online gaming that involves prize money are more prone to hacking. We think that these hacks are happening to avoid paying fees for the games.
RESEARCH Q4: HYPOTHESES

• We think DoS is the most common form of attack. We anticipate that SQL Injection will be another common form.

• We believe incentives may include financial, as well as publicity purposes.

• We predict that most of these attacks occur in the USA.
RESEARCH Q1: LITERATURE REVIEW

- Many websites and articles have explored vulnerabilities and techniques

- Vulnerabilities include a combination of:
  - Social Engineering
  - Computer Savvy Hackers

- Techniques include:
  - Baiting
  - Elicitation
  - Phishing
  - Spoofing
RESEARCH Q2: LITERATURE REVIEW

Dailymail.com and article by McMullan and Perrier D throws light at online games.

• Famous online games for money making
  • Online Poker
  • Wheel of Fortune
  • Bejeweled

• Hackers entice players with cheat codes that could help them win games

• Players download malwares and viruses on their systems that send their financial data to the author of the malware
Articles on Yahoo news and www.wired.co.uk reports how the online games are being hacked.

- games use credits that players can exchange for real money
- stolen funds are being laundered, unaware senders and receivers are held accountable for the crime
- On May 28th, 2013 7 hackers were charged in a $6 billion money laundering case (Yahoo news)
RESEARCH Q4: LITERATURE REVIEW

CIS journal dated October 2011 informs about the different types of attacks carried out. Some of the most common attacks are:

- DDoS attacks
- SQL Injection

- On August 26, 2013 China Internet Network Information Center reported that the Chinese internet went down due to attacks.

- CloudFlare Chief Executive, Matthew Prince. Mr. Prince said the company observed a 32% drop in traffic for the thousands of Chinese domains
RESEARCH Q1: FINDINGS

- Arhack Forum

<table>
<thead>
<tr>
<th>Social Networking Topics</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>66.89%</td>
</tr>
<tr>
<td>Twitter</td>
<td>4.30%</td>
</tr>
<tr>
<td>Skype</td>
<td>28.72%</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>0.05%</td>
</tr>
<tr>
<td>Flickr</td>
<td>0.03%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hacker Related Posts</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacker</td>
<td>31%</td>
</tr>
<tr>
<td>Non Hacker</td>
<td>69%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hacker Related Posts</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>49.49%</td>
</tr>
<tr>
<td>Twitter</td>
<td>10.74%</td>
</tr>
<tr>
<td>Skype</td>
<td>14.08%</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>100.00%</td>
</tr>
<tr>
<td>Flickr</td>
<td>0.00%</td>
</tr>
</tbody>
</table>
RESEARCH Q2: FINDINGS

- Arhack Threads

- Arhack Posts
RESEARCH Q2: FINDINGS

• Shodan Script to find Port 1025

```python
# To find servers with port 1025
from shodan import WebAPI

SHODAN_API_KEY = "72WmLV2f0F1htsp8EdeF5Qvev1v3znxB"

api = WebAPI(SHODAN_API_KEY)

# This example search a specific keyword in Shodan database, and print the results.

try:
    # Search Shodan
    results = api.search("port-1025")
    # Show the results
    print "Results found: %s" % results['total']
    for result in results['matches']:
        print "IP: %s" % result['ip']
        print result['data']
    print ""
except Exception, e:
    print 'Error: %s' % e
```
RESEARCH Q3: FINDINGS

- Anothread

<table>
<thead>
<tr>
<th>postID</th>
<th>TextContent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234</td>
<td>Just extract Sentry, run it, then extract the steam.config (included), then click load snapshot, select the steam.config, save snapshot, load ur combos, proxies, click start and it should start cracking, if it is not then you have no game. Welcome to AI-Adventures®!</td>
</tr>
<tr>
<td>1235</td>
<td>Today, i want to share with you the sites where you can download anything to your mobile phone(s) or Symantec. A visit to these sites will give you the opportunity to download games, music, etc.</td>
</tr>
<tr>
<td>1236</td>
<td>Hello, i am the new moderator on this site. I will be taking the responsibility for the support, and by that i mean if any of you is in need of assistance on any problems you may have, feel free to me.</td>
</tr>
<tr>
<td>1237</td>
<td>Hello guys, i am sharing this steam hack with you that you can also enjoy these games without paying for them. Instruction is in zip folder, and if it is not let me know i will give u again upload a month ago.</td>
</tr>
<tr>
<td>1238</td>
<td>If you ever played simple 2d flash games or similar and struggled with them, you can now make them easier by &amp; quot;cheating &amp; quot; and the way you do that, is by using this tool called Cheat Engine (v.6.2). This is one of the easiest ways to &amp; quot;hack &amp; quot; those kind of games. Cheat Engine works like this: 1. Select the website of the flash game you want to hack in the top left corner (computer icon). 2. Find the value of something e.g. health, money, experience etc. lets say you have 300 coins on a game. 3. Buy something in the game it possible or gain more coins. 4. Input the new value in the cheat engine so that last answer come up (you are looking for the one you are using). 5. Repeat step 1 and 3 till you have no more than 5 answers, preferably 1 to 3 answers. 6. Right click the value and change it (see the tutorial below) to the value you want. e.g. you have 300 coins, so type in 1000000 and then click the box on the left of the value to freeze it so that the value never changes even if you buy something. There are lots of ways to use this and the one i told you was just the basic one. You can find the tutorial on Youtube, this one is a simple one (not made by me) : Spoiler</td>
</tr>
</tbody>
</table>
RESEARCH Q3: FINDINGS

• Hackhoundthread

Cyberghost has a free and paid service. The free service is good, I have the paid service. I would suggest you purchase it. With Cyberghost, you're establishing your online privacy and internet freedom with a few clicks. No exhausting searches for new, overpowered and in the end slow web proxies anymore and no crazy and complicated browser settings needed. And the best thing: You're not limited to your browser to use the web anonymously. You can also use any other program on your PC with access to the Internet. Like your messenger (ICQ, XFire, Skype, etc.), your download clients, and games (World of Warcraft, etc.).

Homepage: http://cyberghost.org/
RESEARCH Q4: FINDINGS

- Attack Stats

![Chart showing attack stats](image-url)
RESEARCH Q4: FINDINGS

• Shodan Script to Extract Related Attacks:
  • Source of attack
  • Description of attack
  • Date of attack
  • Authors of attack
RESEARCH Q4: FINDINGS

• Source Map
REFERENCES

- https://www.acunetix.com/websitesecurity/xssfacebook/
- http://www.theguardian.com/uk-news/2013/nov/08/gambling-machines-drug-money-laundering-bookies