Cybersecurity Bootcamp Report: Google Dorking Fun!

Name: [LINTO BABY]

This report details a cool, hands-on exercise I conducted during the bootcamp! I dove into Open-Source Intelligence (OSINT), specifically something called Google Dorking. I figured out how everyday search engines can accidentally spill the beans on sensitive info, all because of some simple server or app blunders. It really hammered home how super important it is to set things up securely and handle data carefully!

1. Overview

This part of the report is about a neat little project from the [Name of the Cybersecurity Bootcamp]. I focused on OSINT, and yeah, that means getting into Google Dorking! The whole point was to show how regular search engines can totally help find sensitive stuff that wasn't supposed to be public. This usually happens because of some mix-ups with servers or apps. It just goes to show, keeping things locked down and handling data right is a HUGE deal!

2. Objective

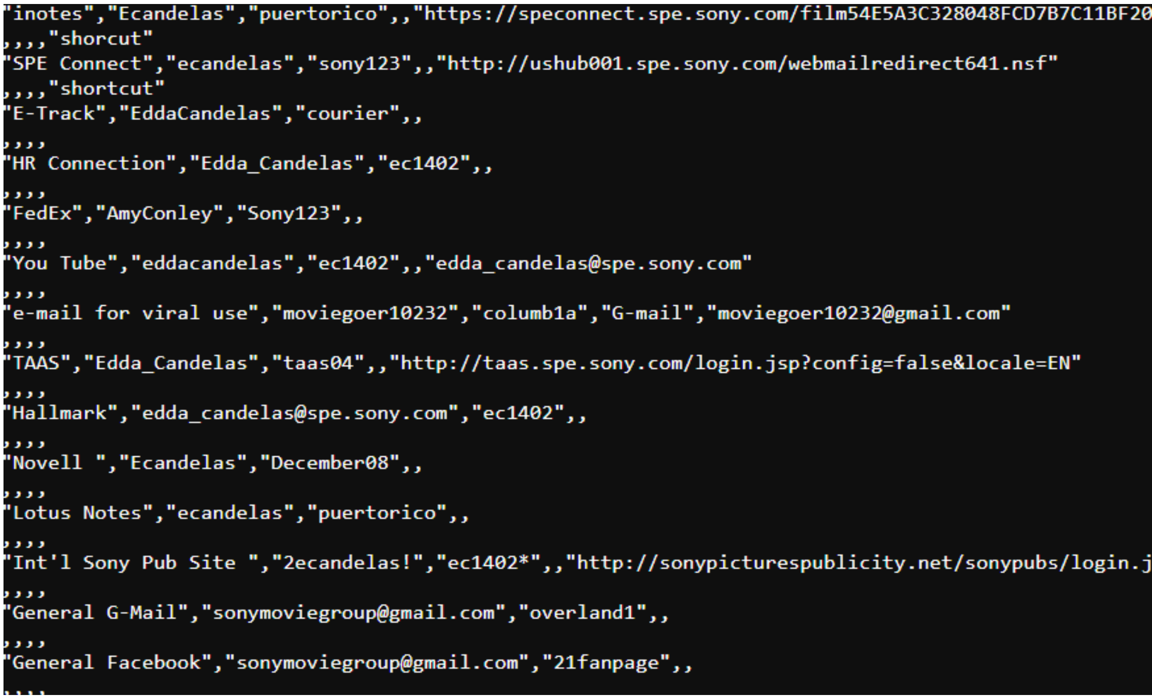
My main goal? To pinpoint data sitting out in the open that was never meant for public eyes! Using some clever Google search tricks (yep, those 'dorks'!), I played detective, pretending to be someone trying to snoop around. I wanted to see firsthand just how simple it could be to uncover weak spots like misconfigured web servers, exposed directories, or even leaked passwords. Talk about eye-opening, huh?!

3. Findings

I found some pretty interesting (and a bit scary!) stuff just by using Google Dorking. It really showed me how much sensitive info can accidentally get out there!

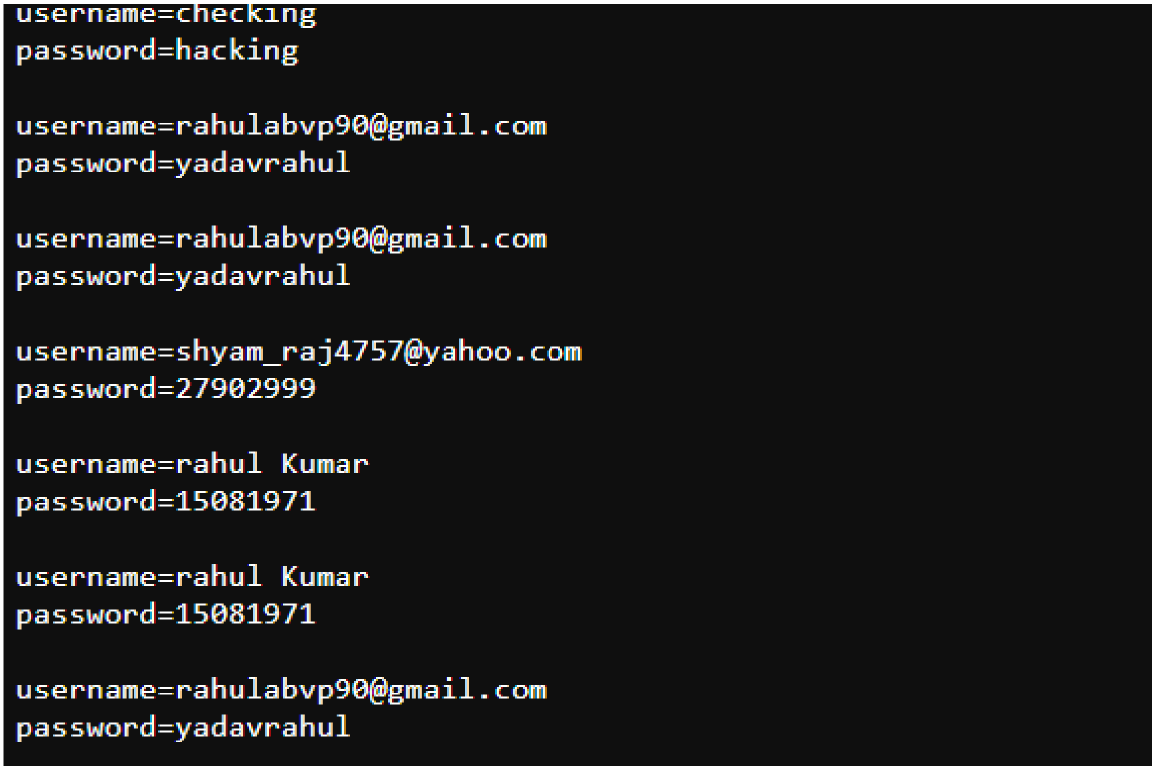
- **My Go-To Google Dork:**
    1. `intext:"confidential" filetype:txt intext:"@gmail.com"` - This was a super handy trick! It helped me find plain text files that actually had the word "confidential" in them, plus a Gmail address. That's usually a big hint that it's internal chat or some other sensitive tidbit.
- **My Top 3 "Aha!" Moments:**

1. **Oops! Usernames and Passwords Out in the Open! (Check out this link: https://wikileaks.org/sony/docs/bonus/1/Password/Digital%20User%20Name%20and%20passwords.txt)**
   - **What I found:** This was probably the biggest shocker! I found a simple text file that seemed to have usernames and passwords just sitting there. Now, this specific one was from a known leak (thanks, WikiLeaks!), but finding it with Google Dorking really shows how easily super important login info can get exposed if a live system isn't careful. It's a huge reminder about how bad data breaches can be and why keeping passwords safe is a must!
   - **Screenshot:**



```
"inotes","Ecandelas","puertorico",,"https://speconnect.spe.sony.com/film54E5A3C328048FCD7B7C11BF20
,,,,"shorcut"
"SPE Connect","ecandelas","sony123",,"http://ushub001.spe.sony.com/webmailredirect641.nsf"
,,,,"shortcut"
"E-Track","EddaCandelas","courier",,
,,,,
"HR Connection","Edda_Candelas","ec1402",,
,,,,
"FedEx","AmyConley","Sony123",,
,,,,
"You Tube","eddacandelas","ec1402",,"edda_candelas@spe.sony.com"
,,,,
"e-mail for viral use","moviegoer10232","columb1a","G-mail","moviegoer10232@gmail.com"
,,,,
"TAAS","Edda_Candelas","taas04",,"http://taas.spe.sony.com/login.jsp?config=false&locale=EN"
,,,,
"Hallmark","edda_candelas@spe.sony.com","ec1402",,
,,,,
"Novell ","Ecandelas","December08",,
,,,,
"Lotus Notes","ecandelas","puertorico",,
,,,,
"Int'l Sony Pub Site ","2ecandelas!","ec1402*",,"http://sonypicturespublicity.net/sonypubs/login.j
,,,,
"General G-Mail","sonymoviegroup@gmail.com","overland1",,
,,,,
"General Facebook","sonymoviegroup@gmail.com","21fanpage",,
,,,,
```

2. **Whoops! An Internal System File Exposed! (Take a peek here: http://www.fundflowmanagers.com/mns.txt)**
   - **What I found:** I stumbled upon a plain text file that looked like an internal system file or maybe even a list of files on a server. When these kinds of files are just out there for anyone to see, it's a classic sign that someone messed up the server settings. It gives away secrets about how a system is set up or what data it holds, which is exactly what a bad guy would want to know!
   - **Screenshot:**



```
username=checking
password=hacking

username=rahulabvp90@gmail.com
password=yadavrahul

username=rahulabvp90@gmail.com
password=yadavrahul

username=shyam_raj4757@yahoo.com
password=27902999

username=rahul Kumar
password=15081971

username=rahul Kumar
password=15081971

username=rahulabvp90@gmail.com
password=yadavrahul
```

3. **Yikes! An Internal Email Just Hanging Out! (See it here: `https://irtfweb.ifa.hawaii.edu/~s2/software/iarc/1305/130516-email-from-CL.txt`)**
   - **What I found:** This was an internal email, just a text file, sitting on a public server. Even if the email itself wasn't super dramatic, the fact that internal conversations are publicly accessible via a direct link is a big red flag for a misconfigured system. Stuff like this can leak all sorts of info, helping attackers plan sneaky tricks like phishing or just gather more intel.

4. Risks Identified

So, what's the big deal with all these Google Dorking finds? Well, they really highlight some major headaches organizations can run into when their data gets out there by accident:

- **Data Leaks:** Private stuff, like passwords, internal documents, and even private chats, can end up being public. Not good!
- **Easy Access for Bad Guys:** If passwords get out, it's like handing over the keys to the kingdom. Unauthorized access, here we come!
- **Attackers Get Smarter:** When internal files and emails are public, it's like a free cheat sheet for bad actors. They can use that info to pull off even nastier tricks like phishing or social engineering.

- **Reputation Takes a Hit:** If sensitive data gets exposed, people lose trust in the company. That can really hurt their image with customers and partners.
- **Legal Trouble & Fines:** Oops! Exposing data can also mean breaking privacy rules (like GDPR or HIPAA), which can lead to big legal problems and hefty fines. No fun there!

5. Conclusion

Wrapping things up, this Google Dorking adventure in the cybersecurity bootcamp was seriously eye-opening! It gave me a real feel for how crucial it is to set up systems securely and be super careful with information. It clearly showed me that even small mistakes in configuration can lead to super sensitive, confidential data getting out there, creating huge security headaches. Being able to spot these kinds of vulnerabilities using OSINT is a must-have skill for anyone in cybersecurity. It just screams that we need to keep an eye on things constantly, control who sees what, and do regular security checks to keep our digital world safe and sound!