## PHASE 1 - Recon

In this phase we started by doing enumeration and network hosts discovery with the tool "nmap"

using the following flags = -sV -A -O --script

-sV = this flag shows the running services on the open ports

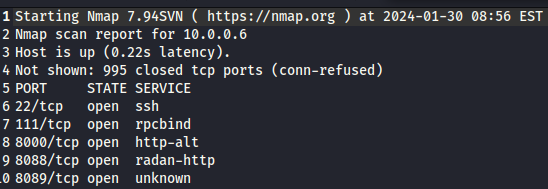
-A = Aggressive scan that makes more noise but gives more information

-O = OS scan to detect

--script = This flag is use to specify a script

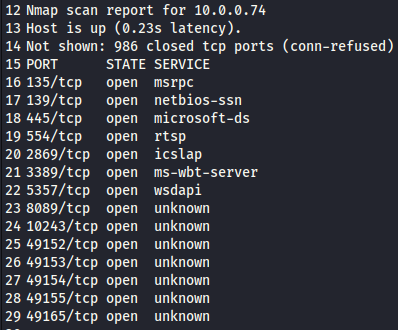
We discovered the following hosts:

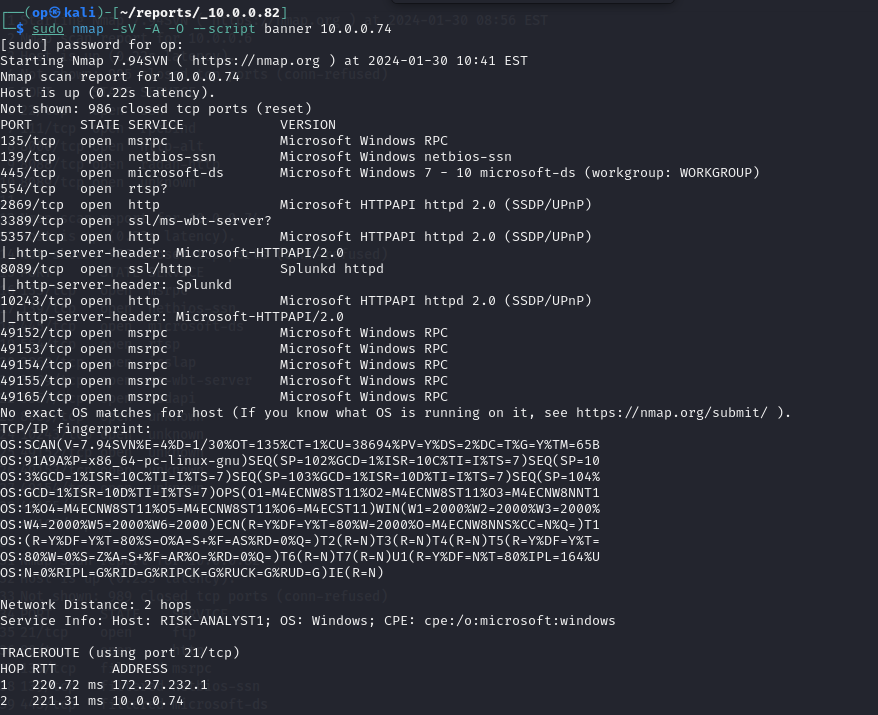
### 10.0.0.6



We identified this host as a SIEM called Splunk this host is out of scope per the client ROE (Rules Of Engagement)

### 10.0.0.74

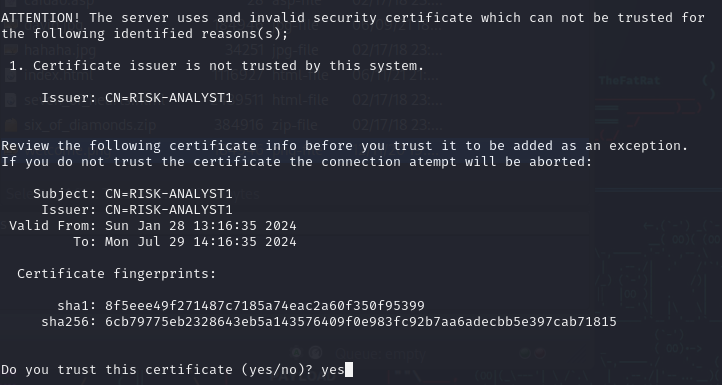


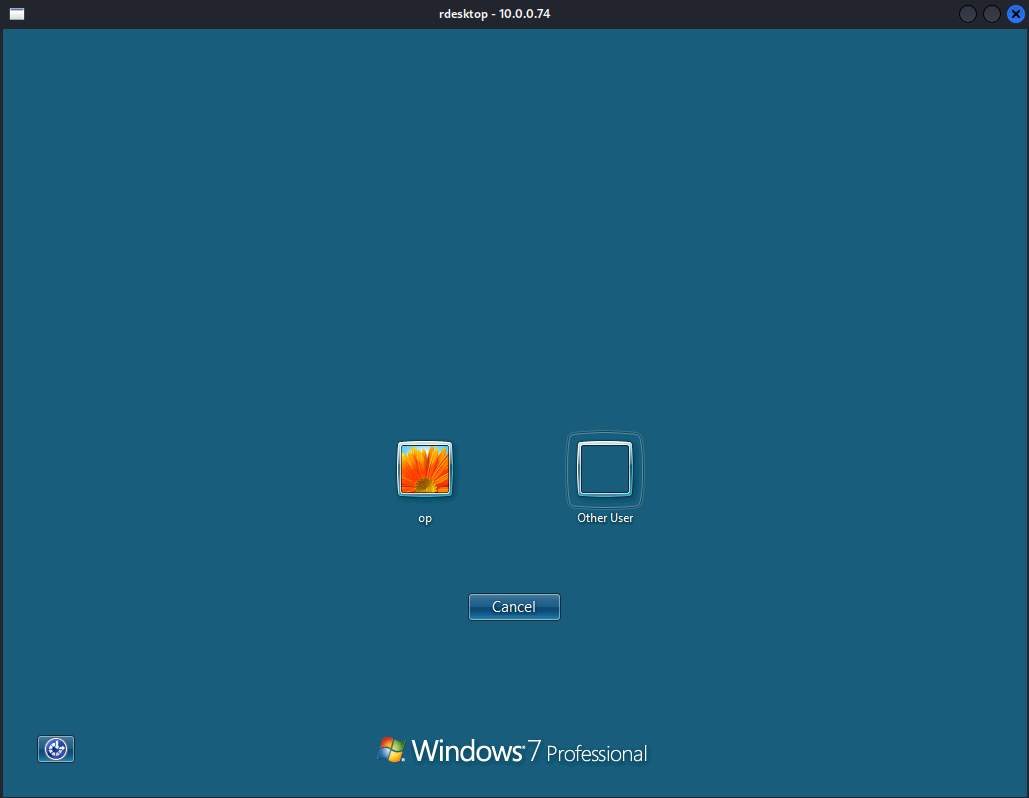


We used the following flags on nmap=

We identified this host that is connected with splunk because it has the port 8089 open and the http header shows Splunkd



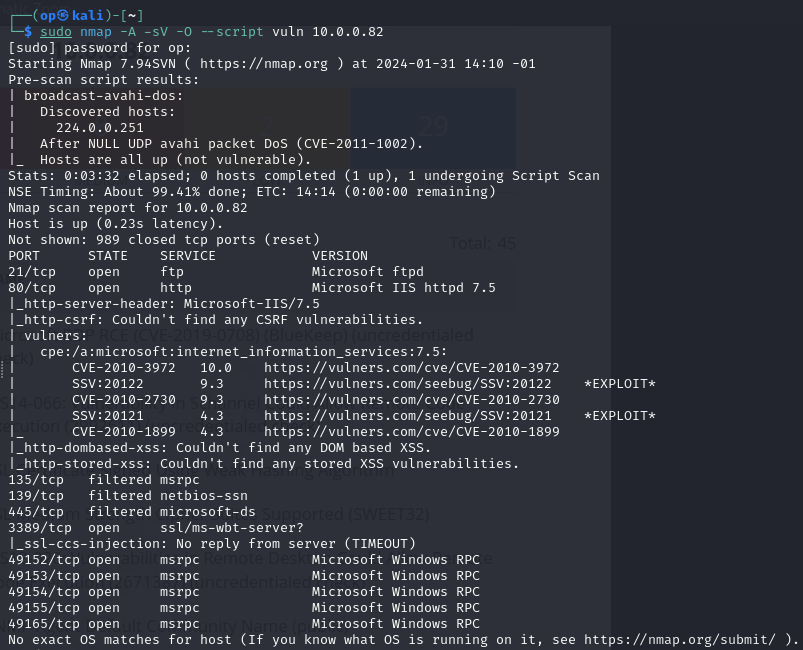


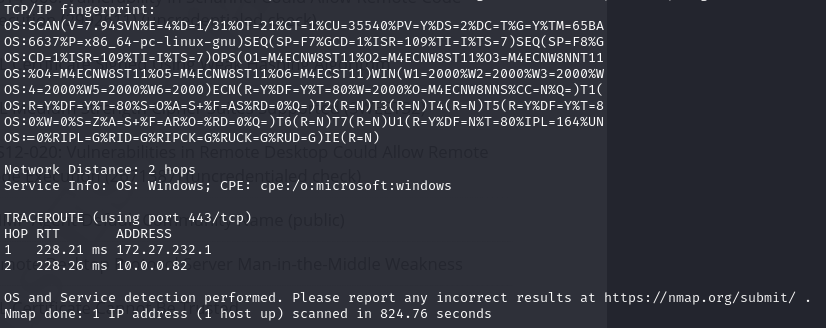


Day 31 / Hour 15:30 We also identified that this host has a RDP port open not requiring username or password to login to it

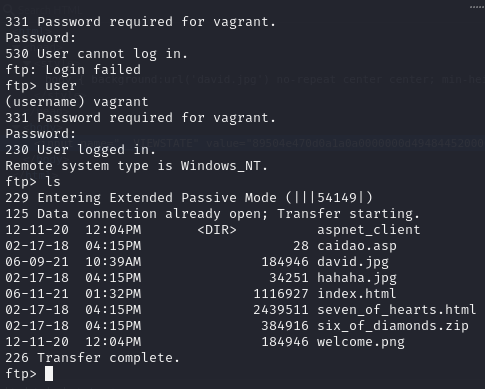
but we got stuck because we don't know the user or the password to login to the machine

### 10.0.0.82

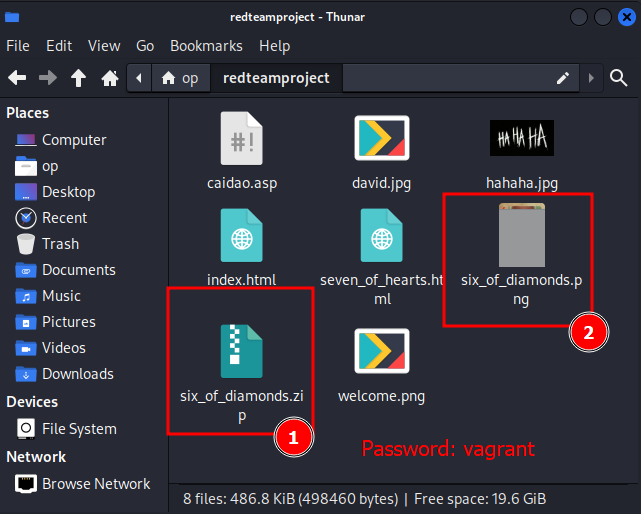




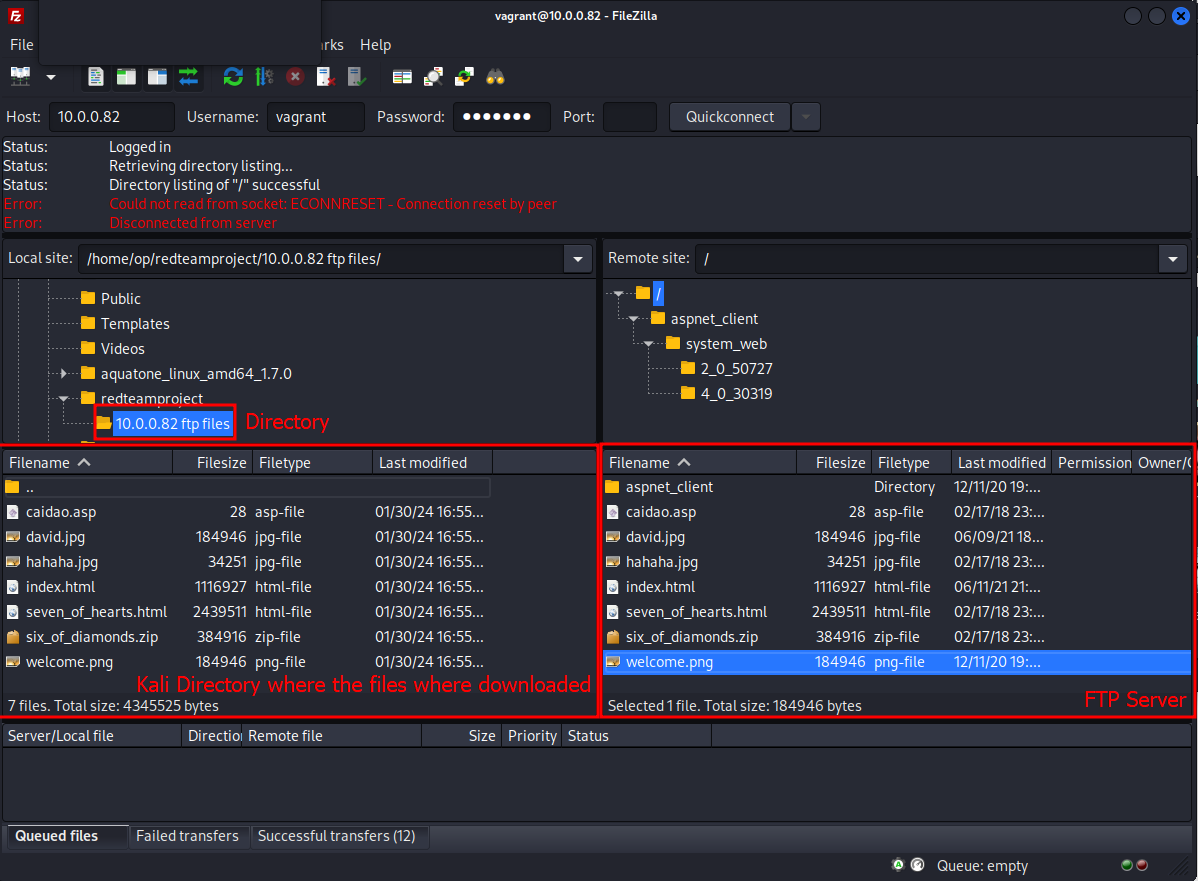
Vulnerabilities scan

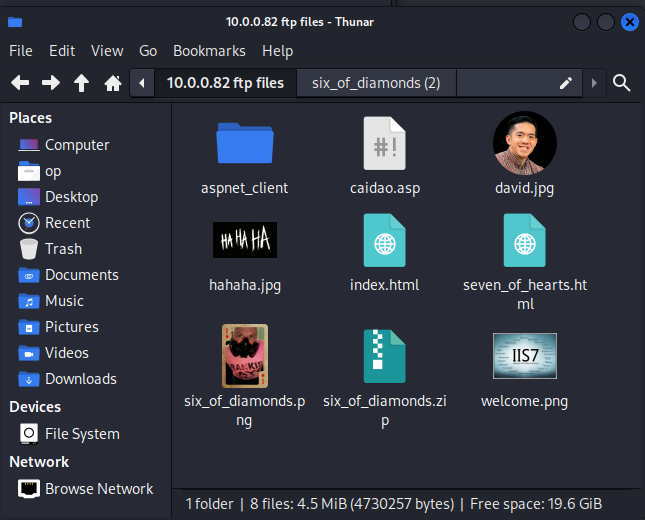


Day 30 / Hour 16:09PM While enumerating we found a ftp port open so we tried to access it but we didnt know neither username or password but later after scanning with nmap using the flag -O we found out the name of the machine in the IP is vagrant, having some knowledge of how ec2 instances work we knew vagrant could also be the username and tried it also for the password and got FTP Access



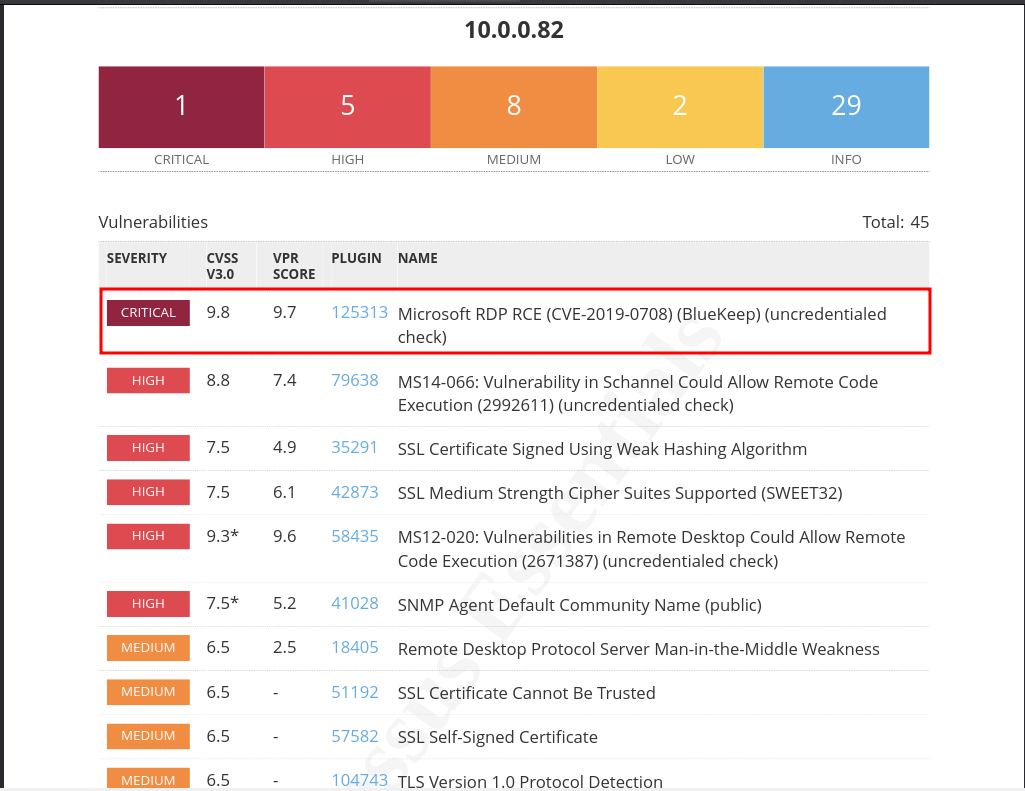
Day 30 / Hour 16:45PM - Was able to guess the ZIP file six\_of\_diamonds.zip password and extract the file six\_of\_diamonds.png, looks damaged/corrupted because it isnt loading properly





Day 30 / Hour 16:56PM deleted the ftp contents downloaded with the terminal and used filezilla instead

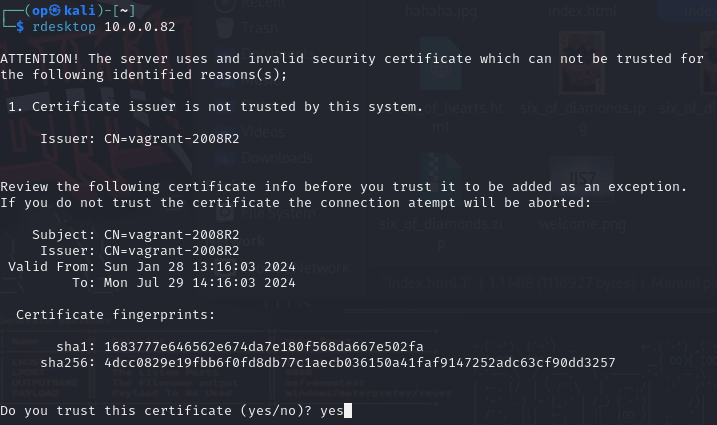
The files are no longer corrupted and can now see the full image from the zip file

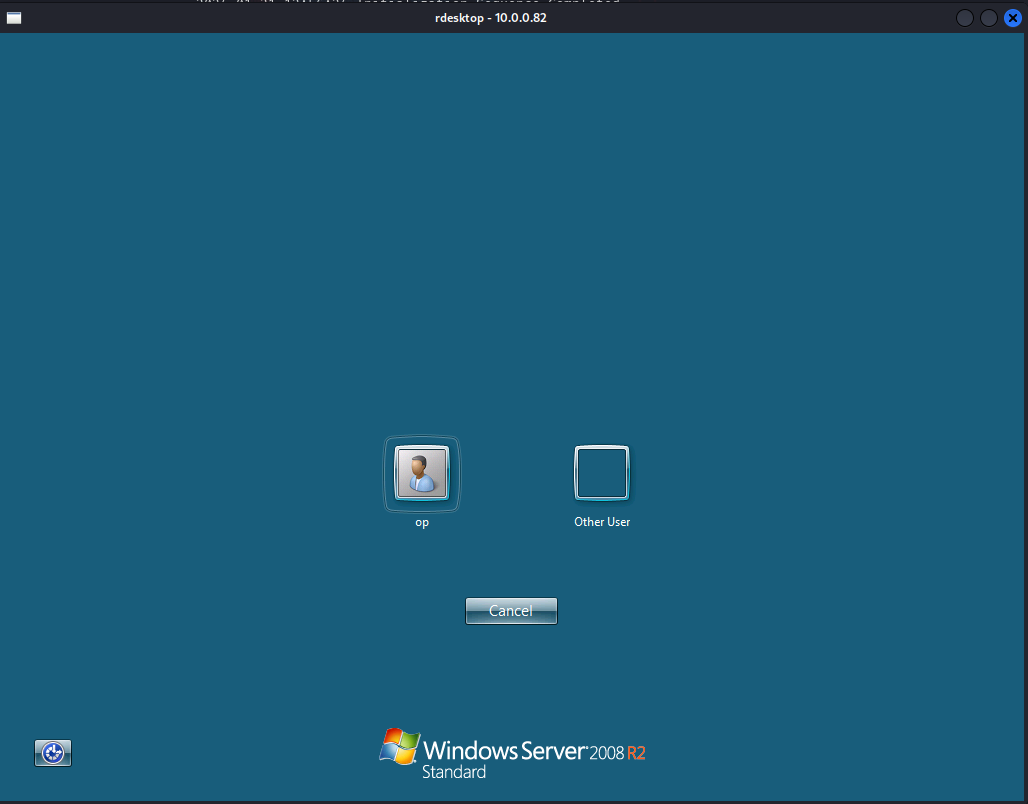


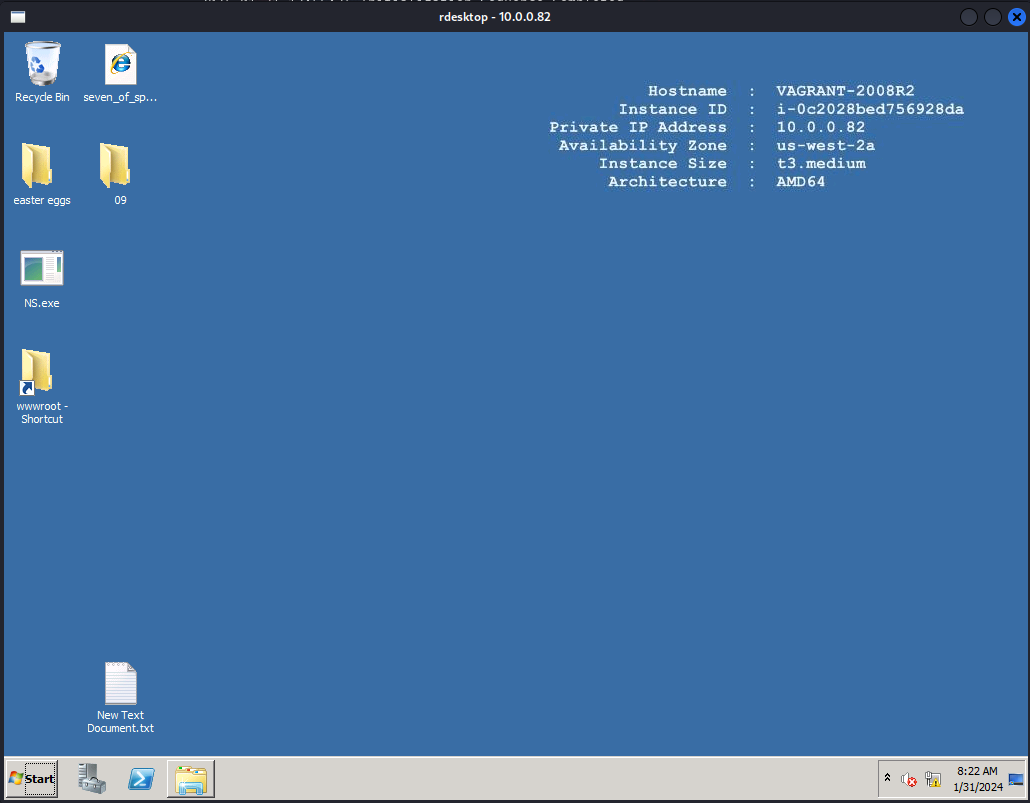


Day 31 / Hour 14:30PM we found a RDP port that escaped us on while enumerating in the day before doing a scan with nessus it showed a critical vulnerability about RDP, we did a nmap scan again and checked the ports and found the port 3389 which is the default port.









After that we tried to connect to the host with "rdesktop" and was successfull!!



