

**Penetration Testing Practical Exam  
01/11/2019**

**James Finglas – B00094138**

Department of Informatics

School of Informatics and Engineering

Institute of Technology Blanchardstown

Dublin 15.

**BN311 Bachelor of Science in Computing**

**Digital Forensics & Cyber Security**

**Penetration Testing**

**01/11/2019**

1: Executive Summary

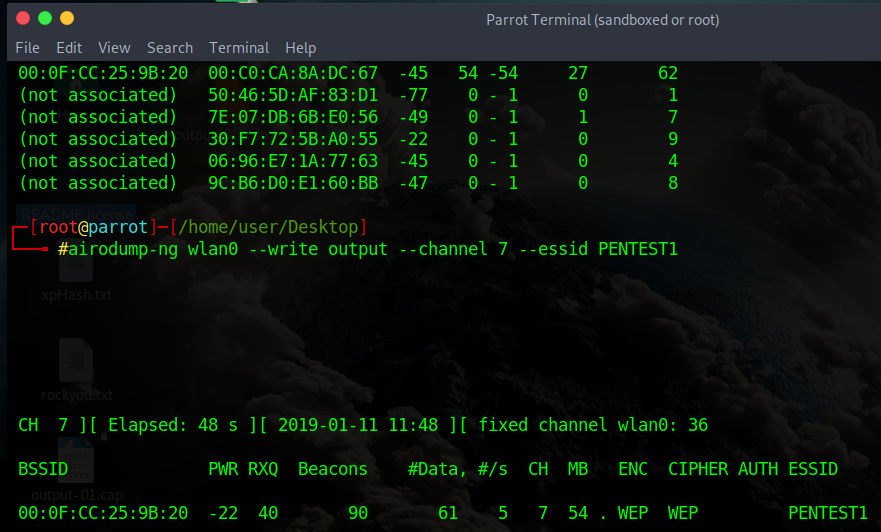
This report documents my activity during this year’s Practical Penetration Testing Exam. I will document the steps taken to data-mine all required information via Open Source Intelligence(OSINT). As well the steps taken to attempt to crack the required WIFI network/s. Finally, I will cover all steps taken and the results of my attempts to penetrate all the machines detected on the given network range.

2: Introduction

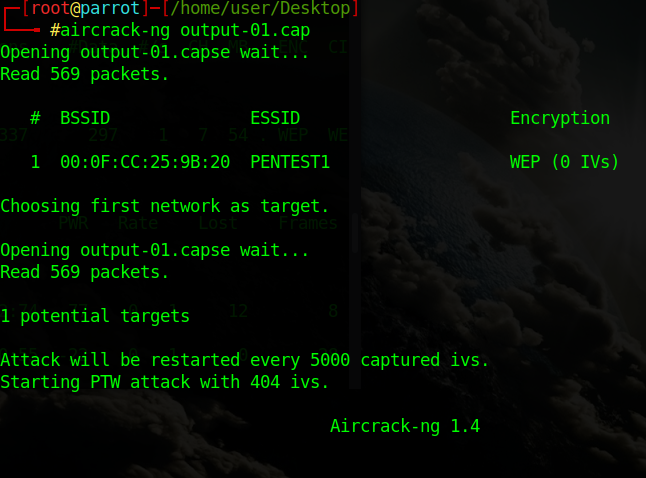
I will begin by attempting to crack WIFI passwords as needed. This can be done along-side OSINT.

# 3: Wifi

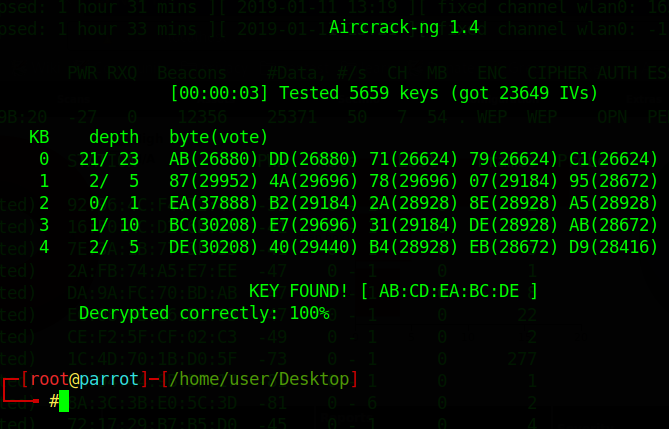
WEP:



*Command used to begin wireless scanning captured to cap file.*

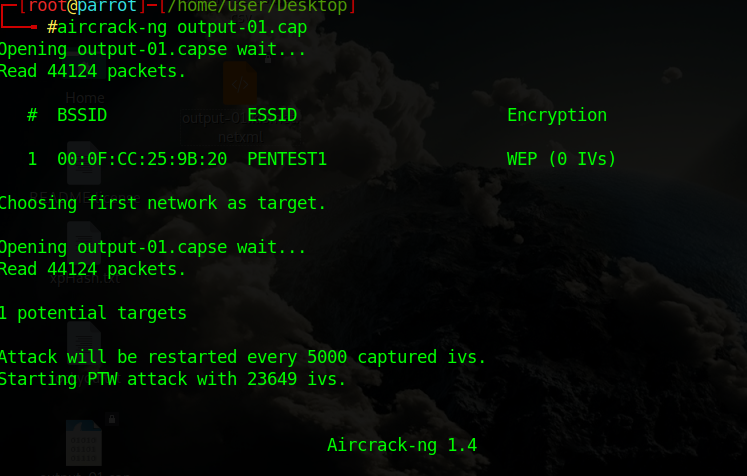


*Command used to attempt to crack capture file for WEP password.*

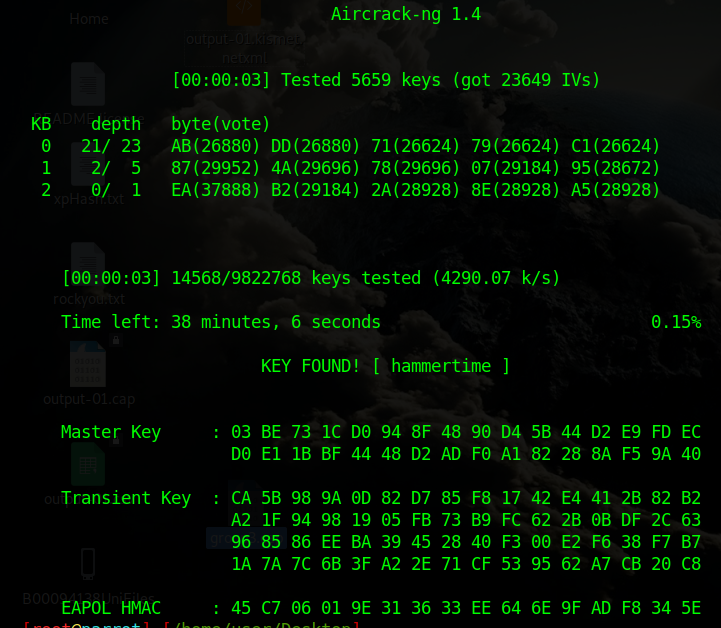
**

*WEP cracked Password.*

WPA:



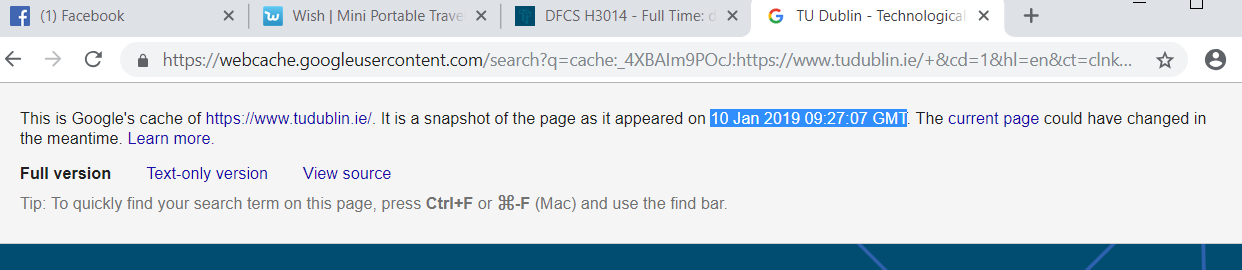
Command used to begin to crack WPA cap file containing handshake.



WPA cap file cracked… password = hammertime.

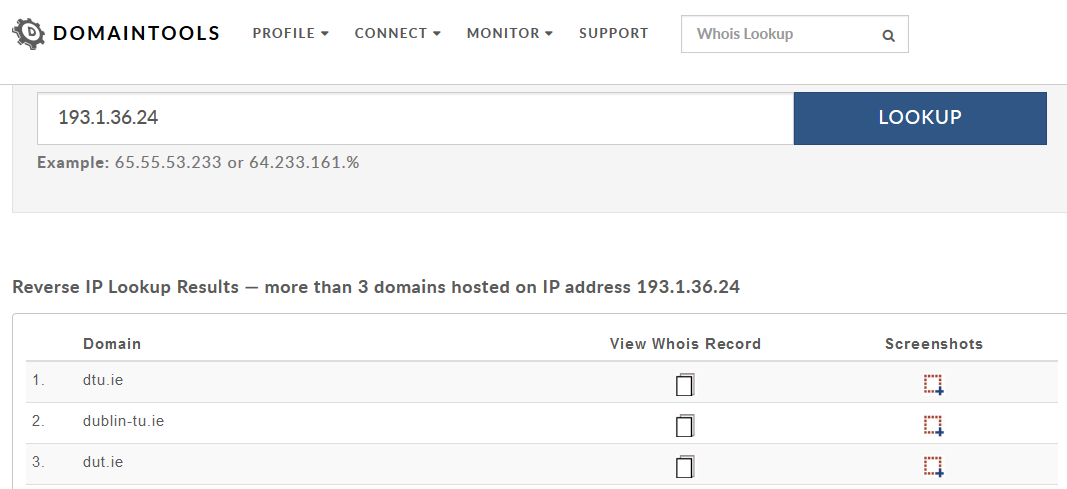
4: Osint (Open Source Intelligence)

Question 1A:



*Screenshot of www.tudublin.ie most recent cache.*

Question 1B:



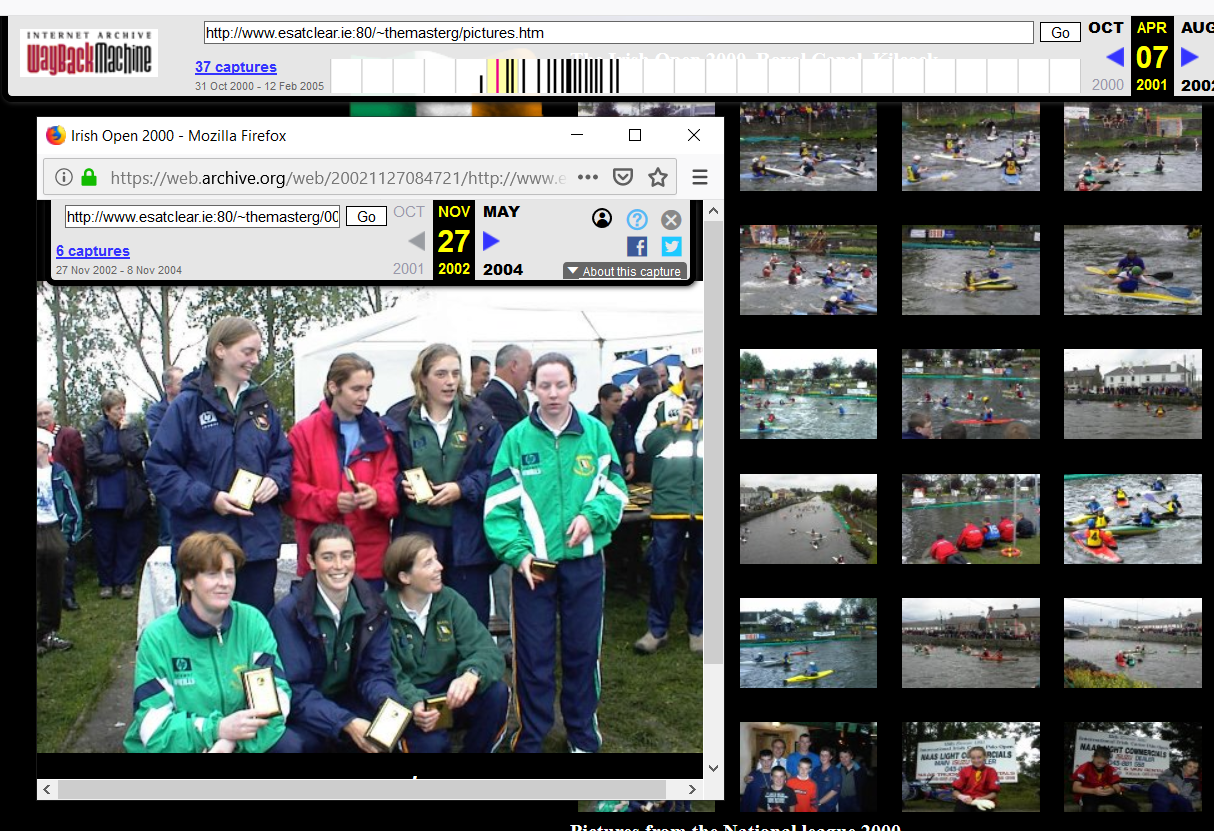
Domains hosted along-side tudublin.ie. More where available but required payment.

Question 1C:



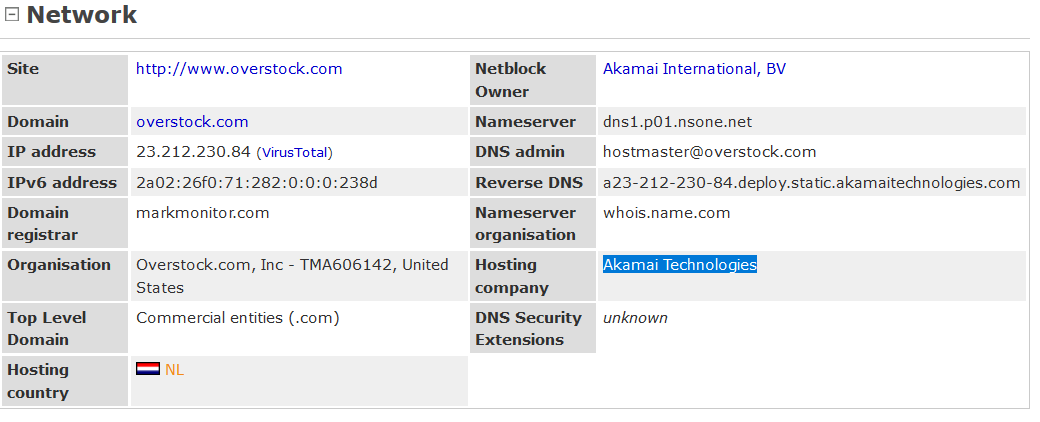
Netcraft appears to be restricted from accessing Operating system data.

Question 1D:

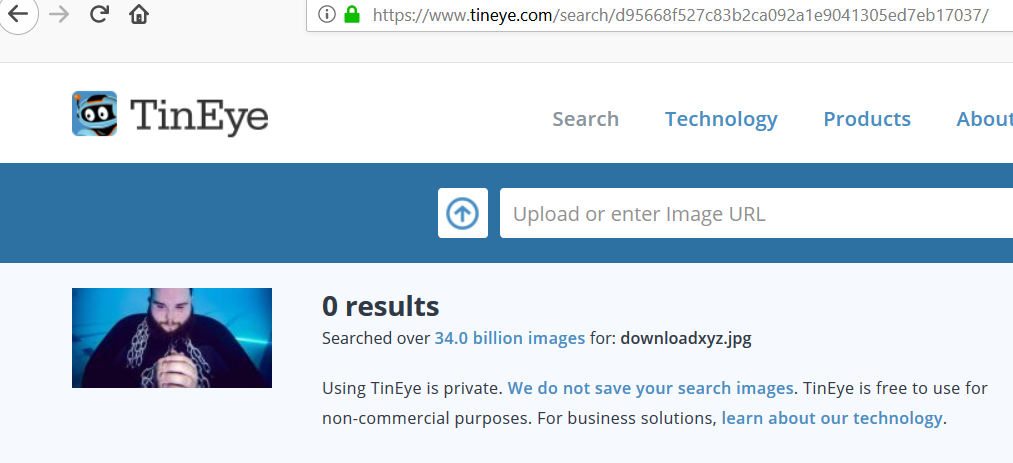


*Womens champs, Irish Open 200o Picture.*

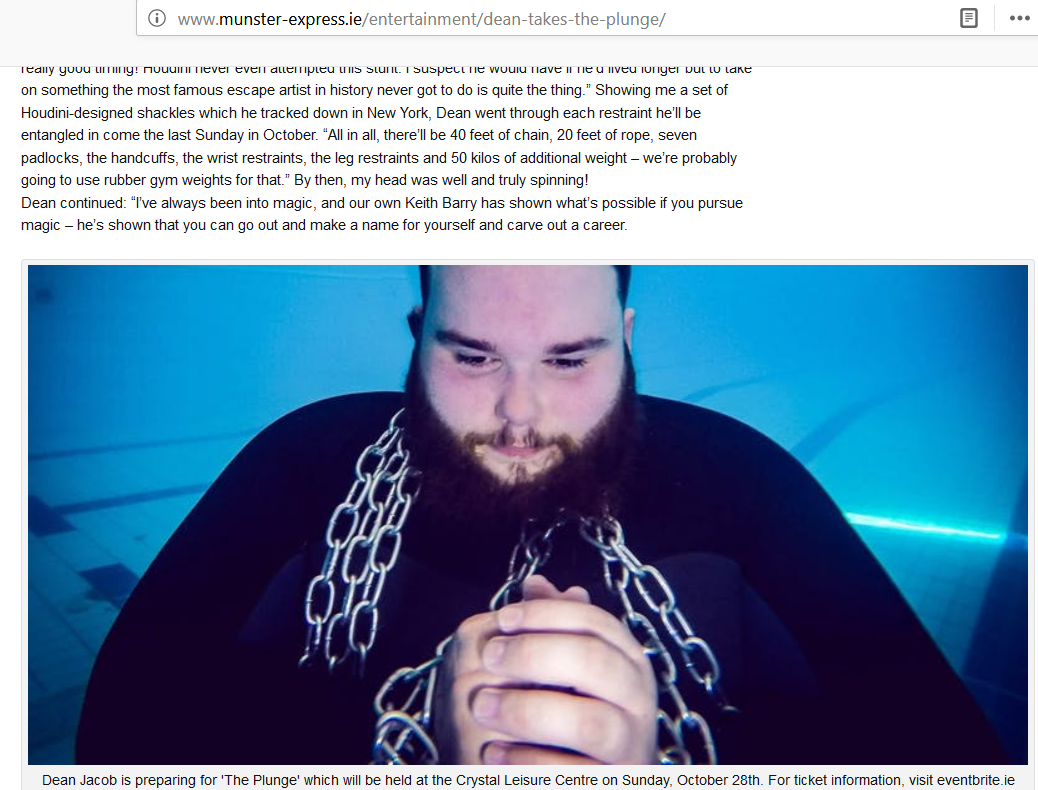
Question 1E:

  
*Hosting company and location.*

Question 1F:



*Tineye failed.*

**

*Appears to have been posted by the munster express online at http://www.munster-express.ie/entertainment/dean-takes-the-plunge/*

# 5: Scanning

Question 1A:

192.168.1.10 windows xp

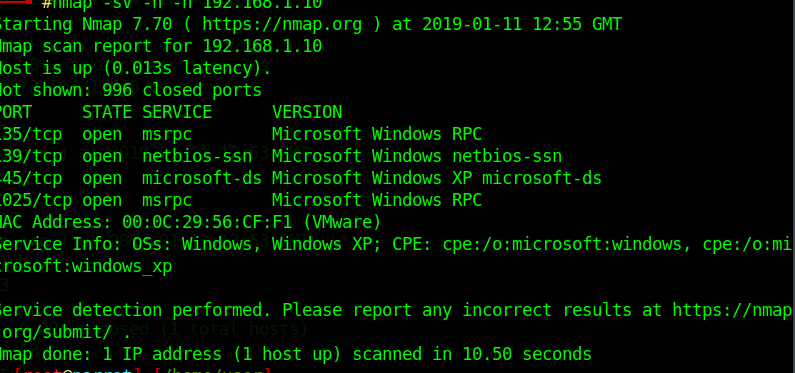
192.168.1.57 linux 2.6.1-2.6.33

192.168.1.110 linux 2.6.13-2.6.32

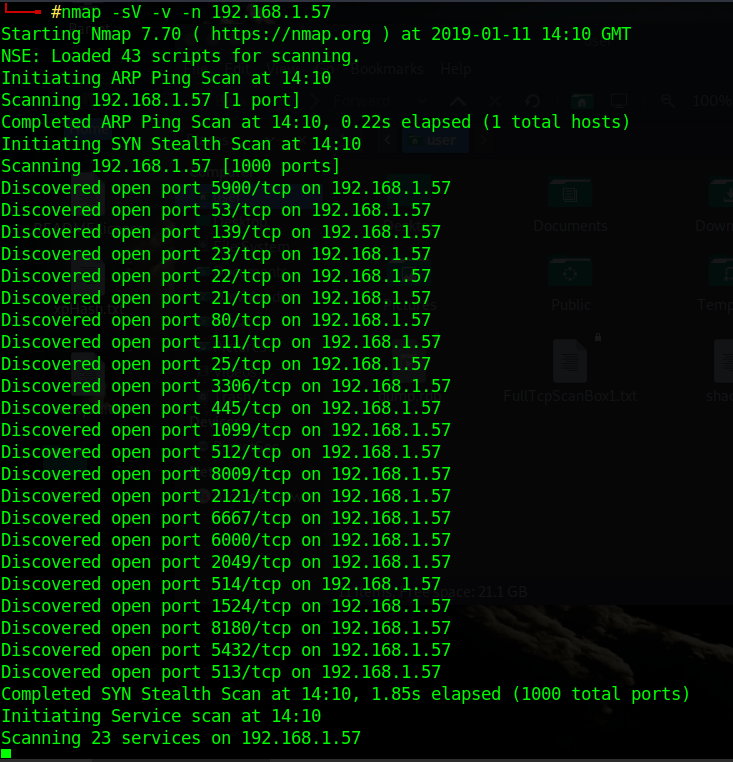
192.168.1.157 FREEBSD 7.0-9.0 RELEASE

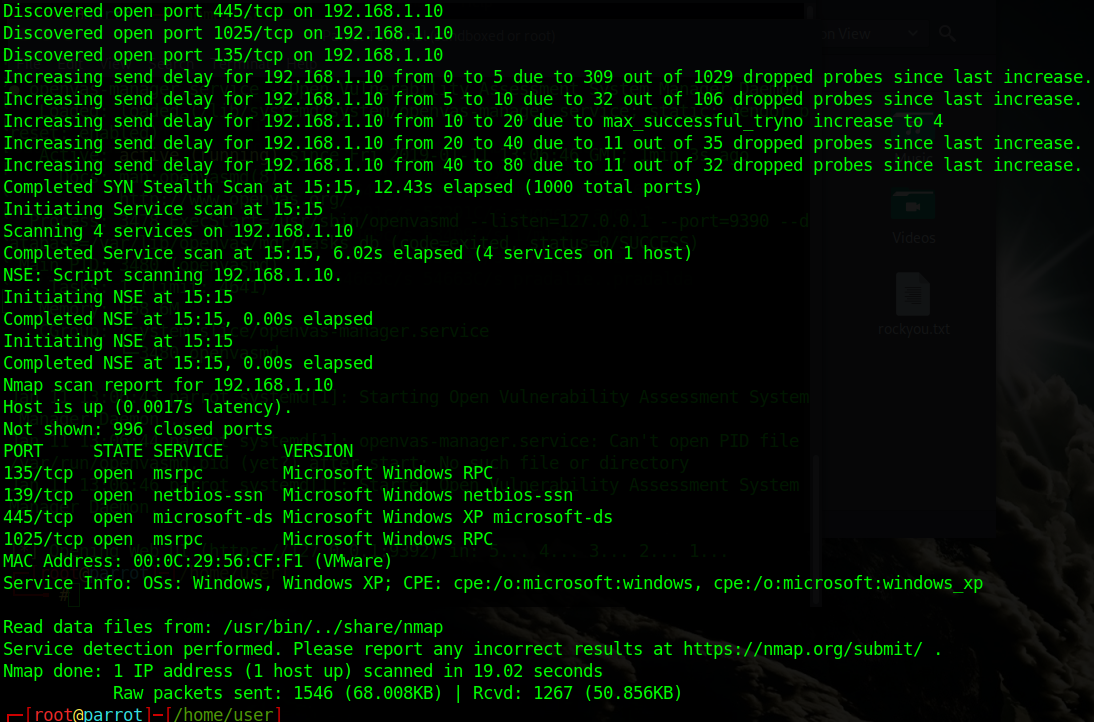
Question 2B:

Box1:

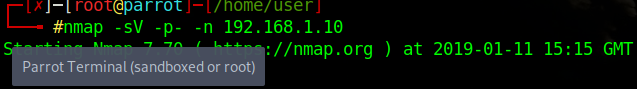


Most common ports of Box1

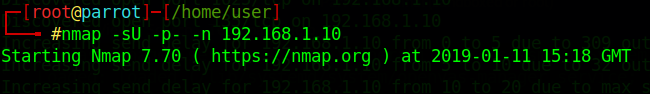




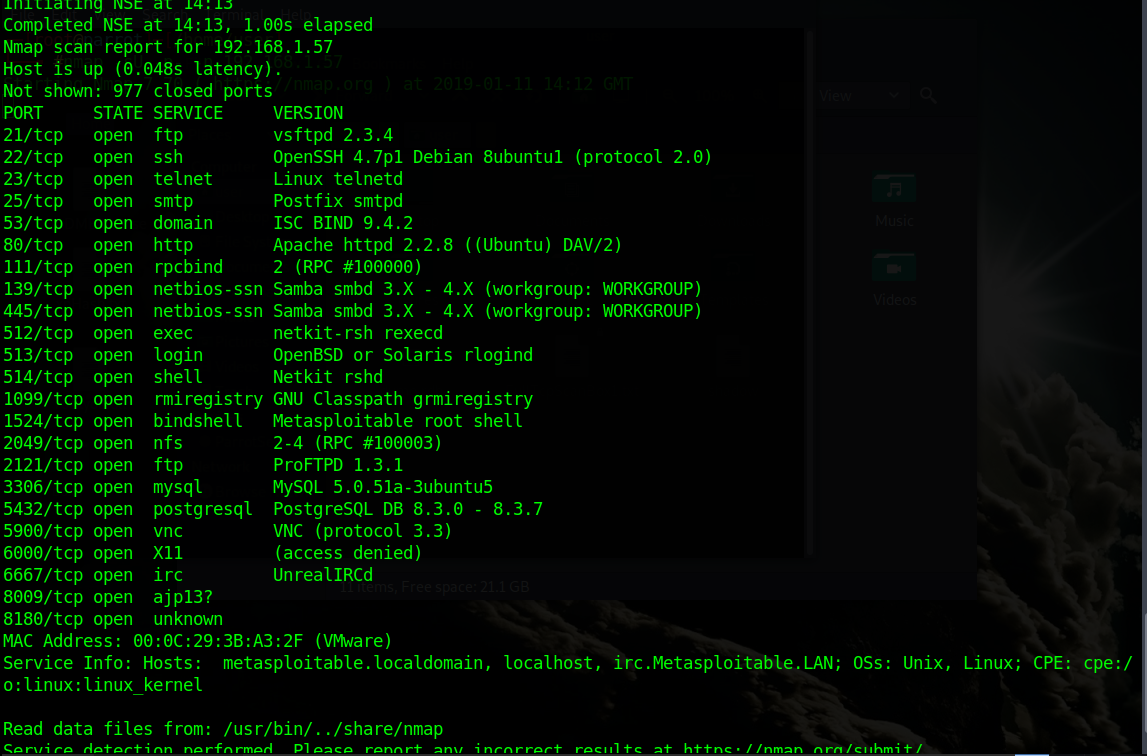
Most common ports for box1.



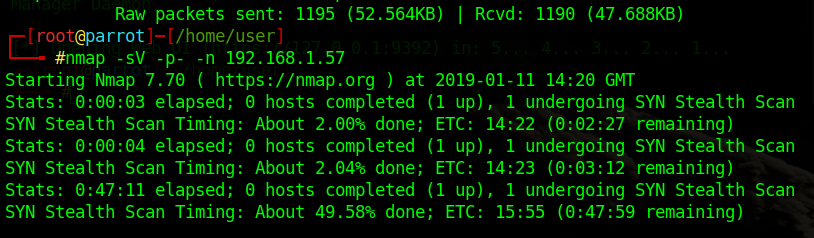
Full tcp scan failed to initialize for box1

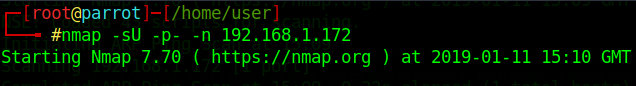


Udp scan for box1.

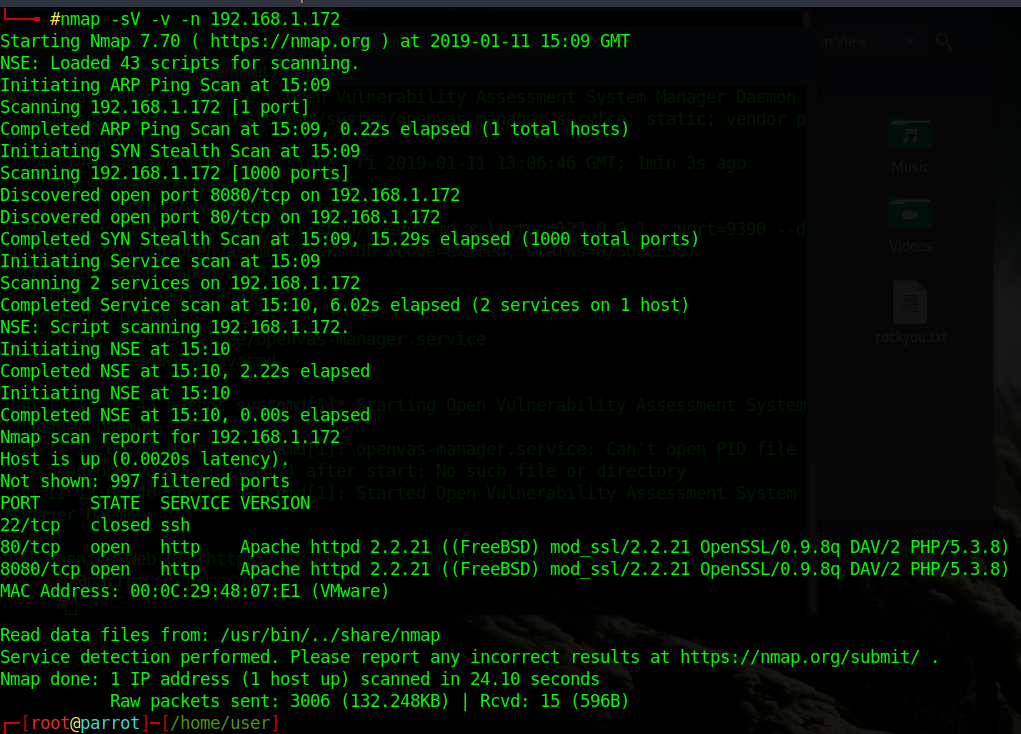


Most common ports for box2.

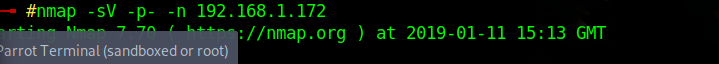


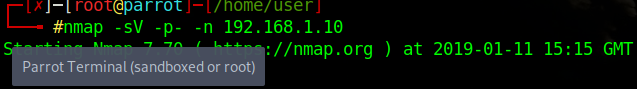
Full tcp scan for box2 simply took too long.

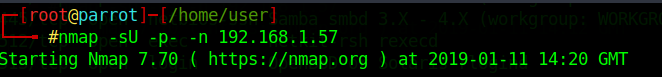
UDP scan for box2.



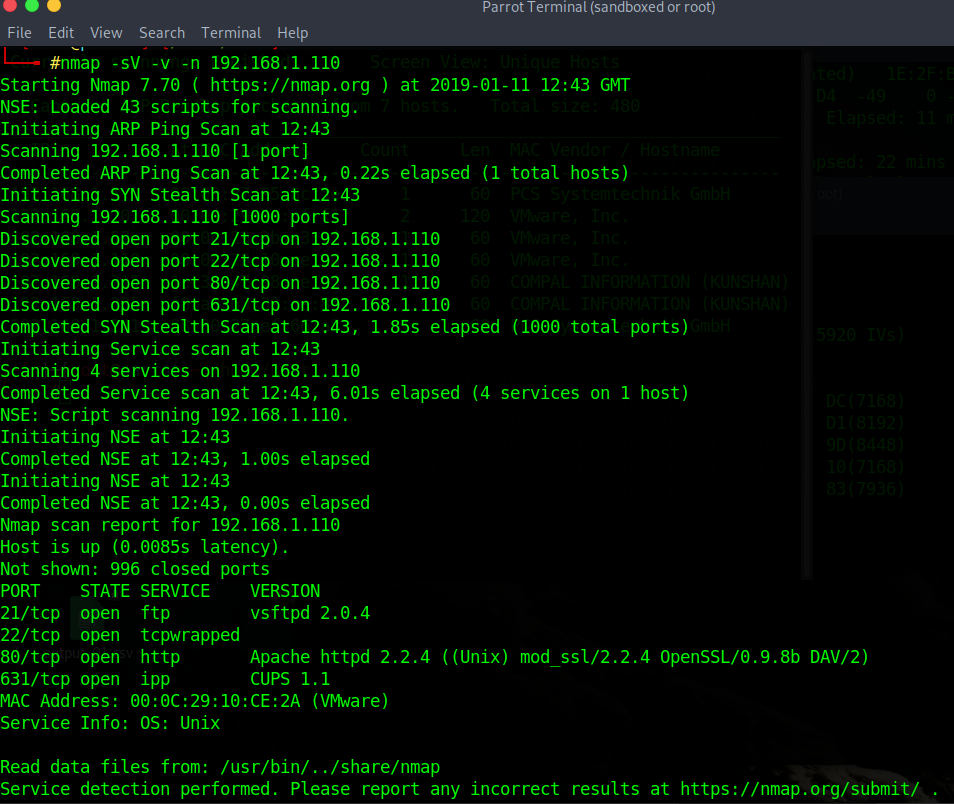
Most common port scan for box4.

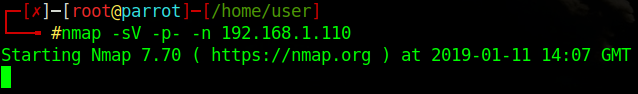


Full tcp scan again failed to initialize for box4

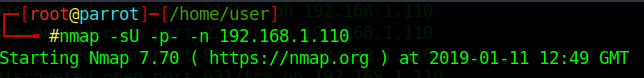


UDP scan for box 4

  
Most common 1000 ports of Box3

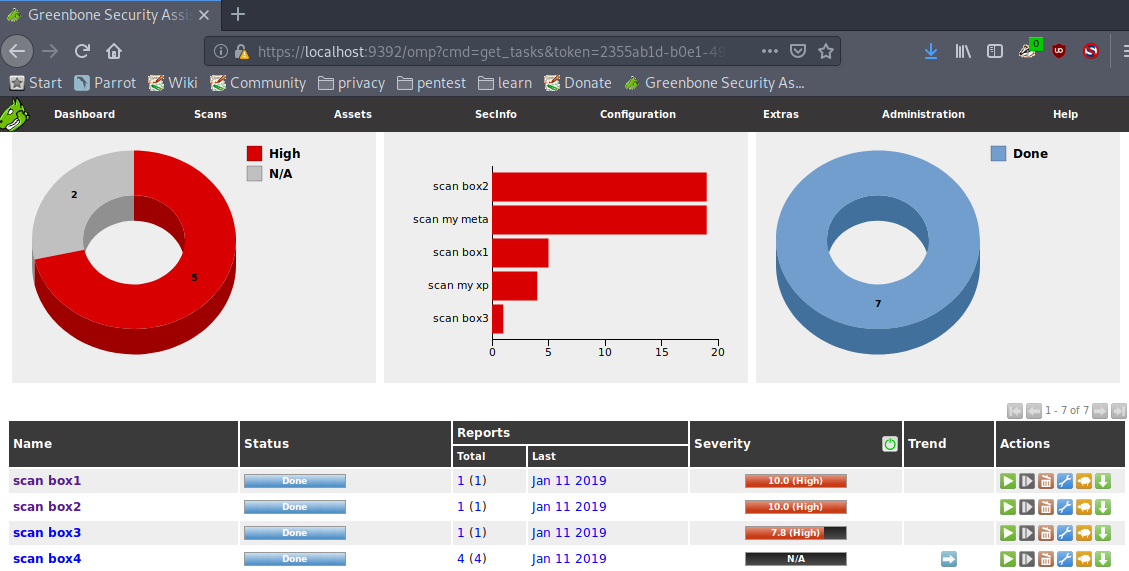


Full TCP would not initiate.



UDP scan of Box3

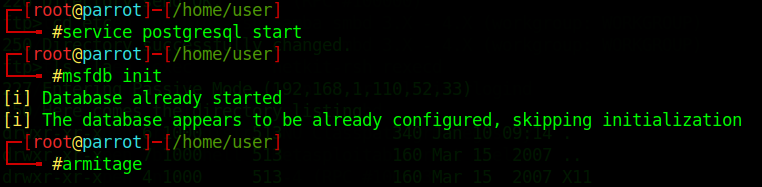
Question 1C:

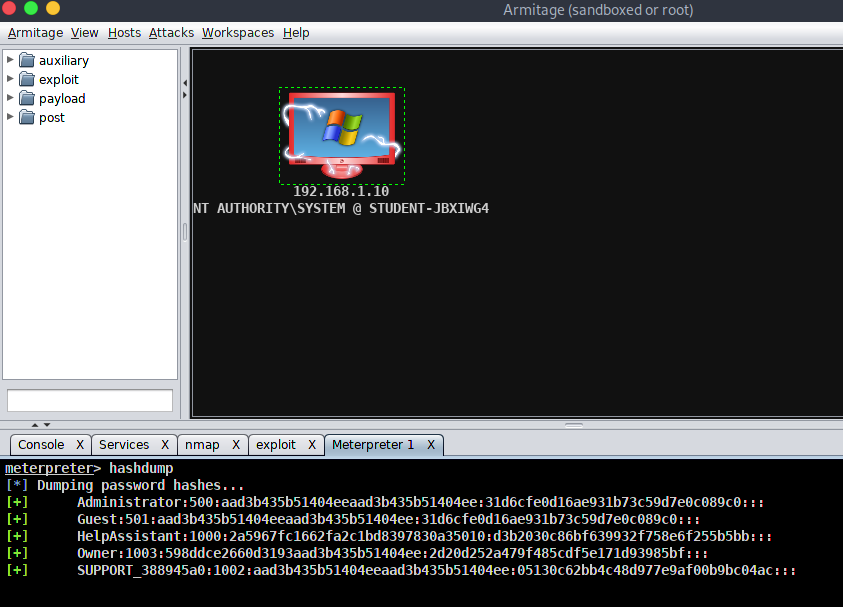


As demonstrated during the Exam, box4 refused to scan, all other boxes scanned fine, PDF’s included in folder along-side the report.

## 5.1: VM1

Begin by launching Armitage. Add host for exp, set os to xp. Find attacks. Launch dcom. Dump hash. I will not be able to crack hash but ill try. Had major difficulties with this so far.





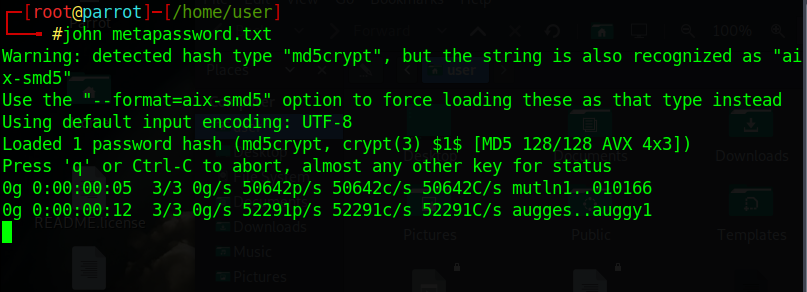
Hash dumped from exploited xp machine at 192.168.1.10. I will not waste time trying to crack as I know it will fail on my machine. Not sure if its due to misconfiguration on my end or not.

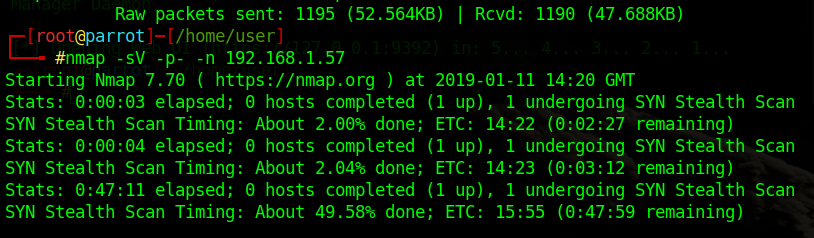
## 5.2: VM2

Vm 2 is metaspolitable2. I logged straight in as root, copied the passwd and shadow file, however due to time restrictions I had to rush my attempt to crack it. So I mere cat the shadow file , pasted to a file and attempted to crack with john real fast.



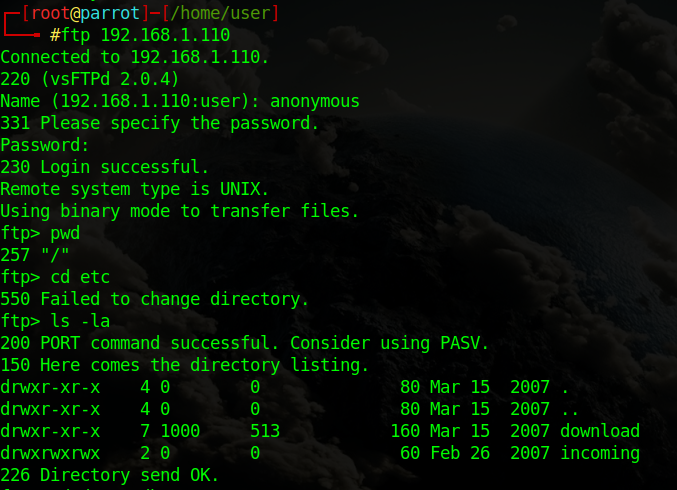
Root access on box 2.



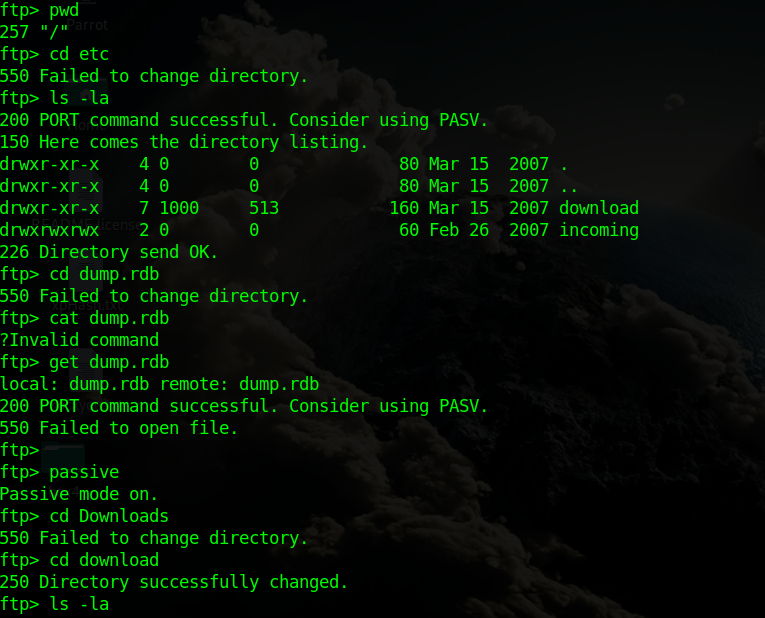
Attempt to crack password with john.

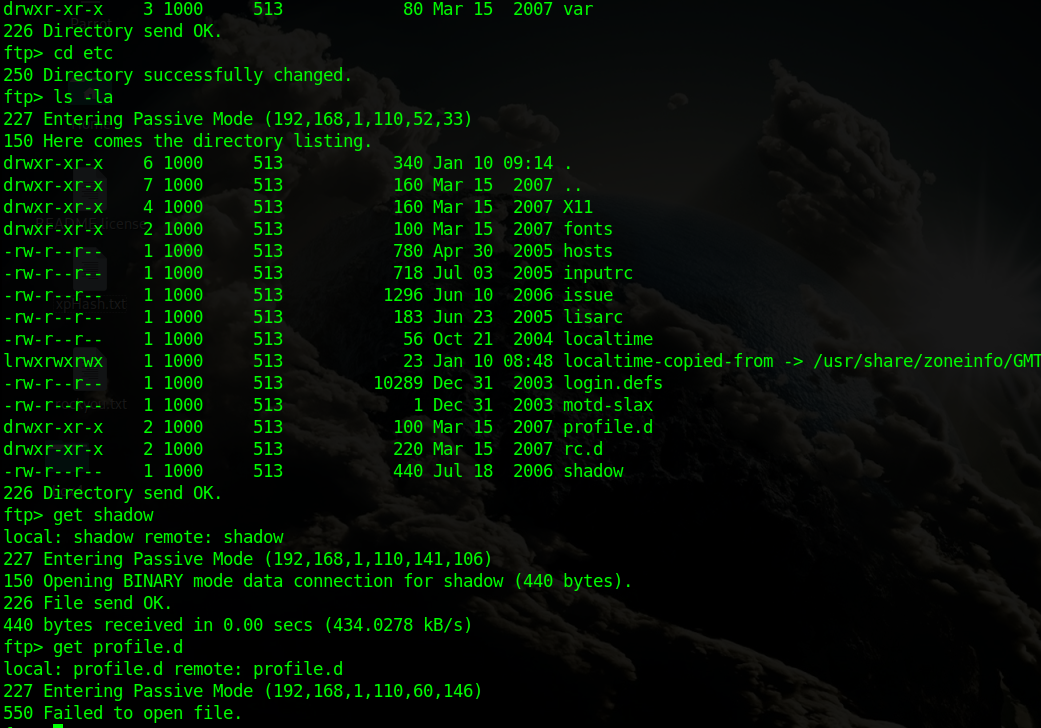
## 

## 5.3: VM3



Connect to box 3 via FTP as anonymous

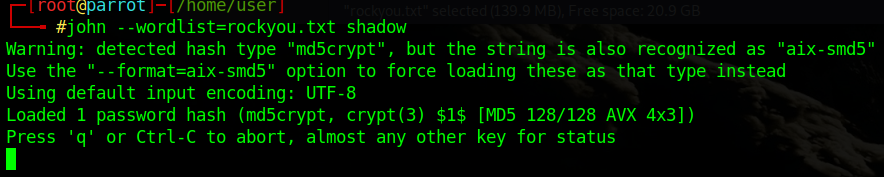


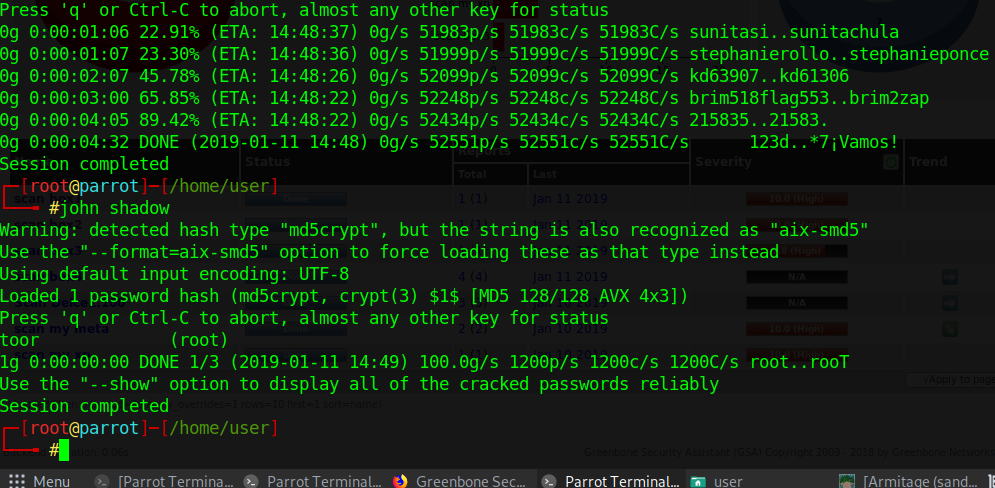


Moved the shadow file over to my machine at home via team viewer and attempted to crack shadow file. This attempt failed. I am not sure why.



Hashcat failed to crack shadow.



Attempting to crack shadow with john on local vm.

Shaodw cracked with john however this is not the right shadow file.

## 5.4: VM4

The address tells me this likely De-Ice 1.110. I will go right after the core file. I will attempt to log in as anonymous FTP.