***PROJECT WORK ON PENETRATION TESTING***

Introduction

Security is one of the topics that gets a lot of attention in today’s world. Because of our increasing reliance on different forms of technology, gadgets, and many other types of systems and devices, more attention is being turned to the topic of how secure and safe these device sand systems actually are. In response to the increase in cybercrimes such as identity theft, information theft, disruption of services, hacktivism, and even the specter of terrorism, many organizations—both public and private—face the challenge of having to test, evaluate, and fix potential security issues before they become the victim of a cybercrime as well as potential lawsuits. It is in response to these situations in the past, present, and future that many organizations are scrambling or pursuing various security solutions.

So enters the penetration tester, who represents one of the best and most effective ways of locating, analyzing, presenting, and recommending strategies to reduce potential risk resulting from security incidents. Pen testers are those people who take their in-depth understanding of technology and its vulnerabilities, as well as strengths, and use them at the request of a client to locate and evaluate security problems before those who don’t have the organization’s best interests at heart.

PURPOSE AND APPROACH

The general purpose to penetration testing toolkits is to minimize the amount of work spent maintaining tools and maximize the amount of time spent performing the test.

So we will be using various tools depending upon requirements.

We will use 4 steps to perform Pentest.

1. Planning and scoping

Here, Main motto is to understand targets and contractors. Resources allocation and budgeting is important. Time, date and engagements are primarily defined. Laws and paper contracts are made here.

2. Info gathering and vulnerability Identification

Systematic attempt to locate, gather, identify and record information about a target. The main aspect here are

* Conducting information gathering
* Performing vulnerability scanning
* Analyzing results of vulnerability scans
* Leveraging information for exploitation
* Weaknesses in specialized systems

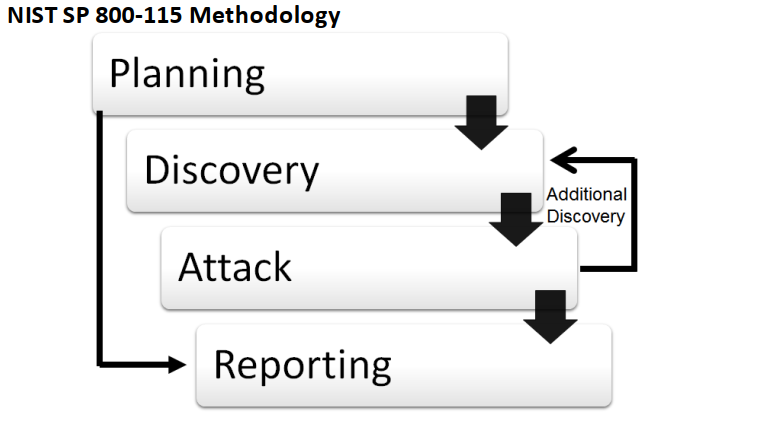
3. Attacks and exploits

Gameplay starts here once information is verified. Things like are performed here;

* Network, wireless/RF, application, and local host exploitation
* Physical security attacks
* Post-exploitation techniques

4. Reporting and communication.

As per obtained result from attack and exploit, reports are made on basis of risk rating and vulnerability assessments. If required solution might be given for them but it is mandatory.



**PROBLEM STATEMENT**

In today’s connected world, everyone benefits from advanced cyberdefense programs. At an individual level, a cybersecurity attack can result in everything from identity theft, to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning.

Security rests on confidentiality, authenticity, integrity, and availability (CAIA)

1. Confidentiality: The concealment of information or resources.

2. Authenticity: The identification and assurance of the origin of information.

3. Integrity: The trustworthiness of data or resources in terms of preventing improper and unauthorized changes.

4. Availability: The ability to use the desired information or resource.

According to clarification I will be doing penetration Testing. I will be checking the vulnerability existed in system and analyze the report of which how secure or weakness exists in system.

***REQUIREMENTS***

We are performing white penetration testing. That means we are provided with all requirements and main aspect *of PERMISSION*.

Nothing performed here are *ILLEGAL*.

We have IP address

1.192.168.0.6

2.192.168.0.7 (Chain)

3. 184.168.139.128 (Target)

Tools are defined as required.

1. NMAP

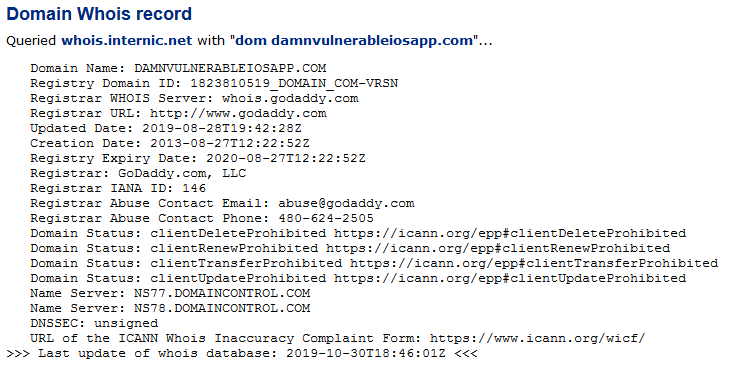
2. NESSUS

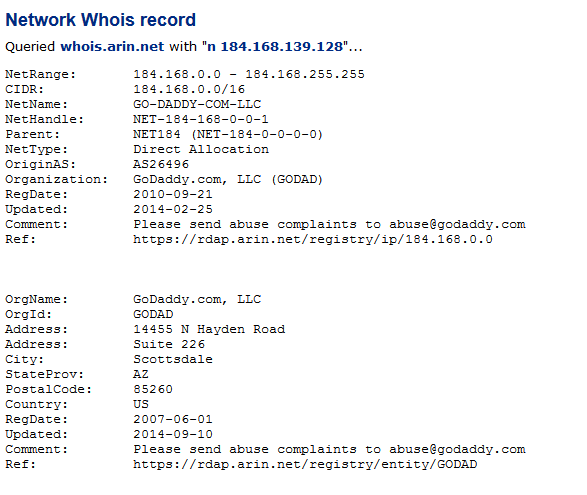
3. DOMAIN DOESSIER ([www.centralops.net](http://www.centralops.net))

4. METASPLOIT

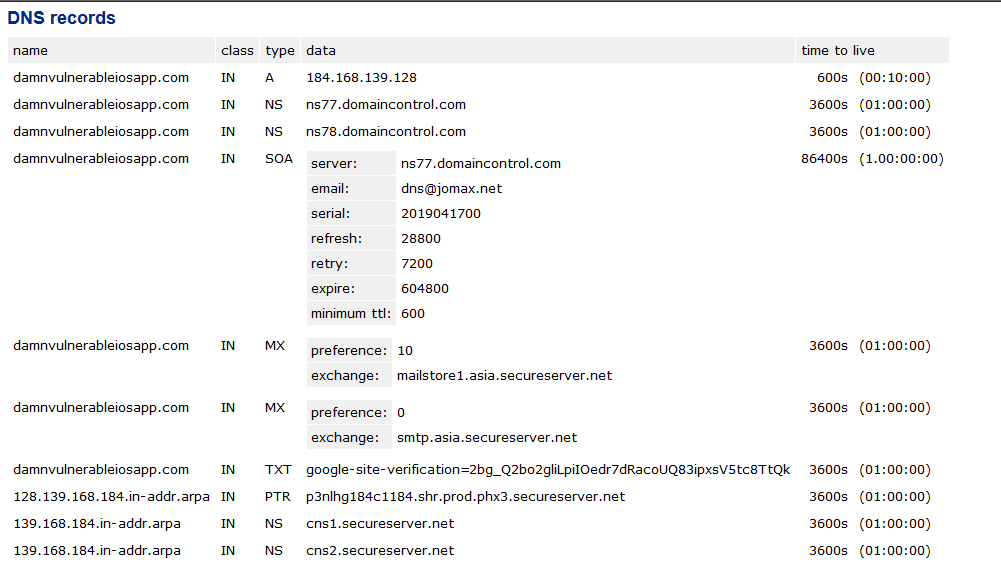
5. LINUX OPERATING SYSTEM.

**ATTACK AND EXPLOITS I**

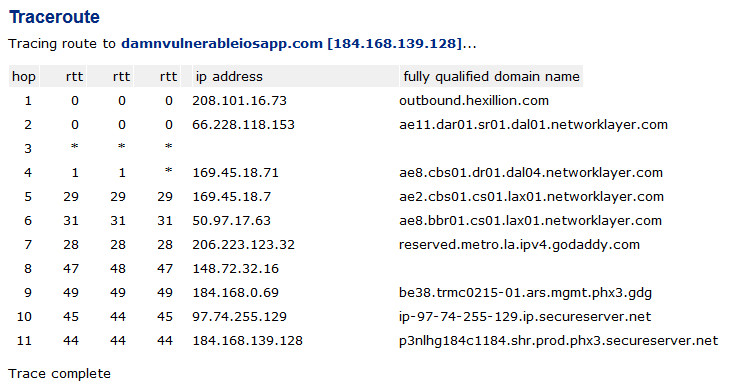




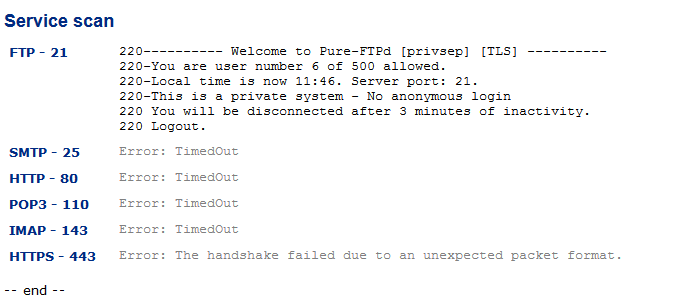
Here we verified its ip range. As per output, it belong to class **B** IP ranges.



Here we can see DNS records like domain owner, their emails, TTL and services provided by them.



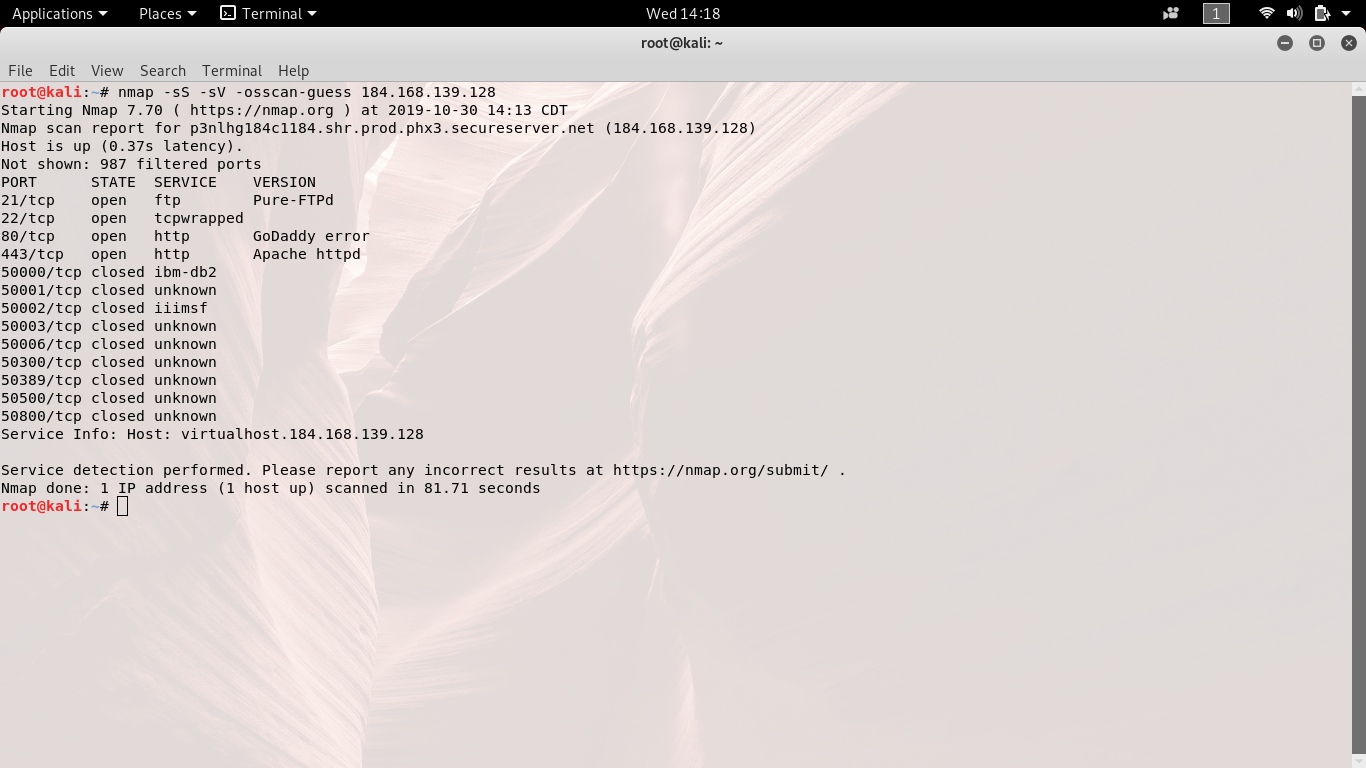
Here we can see how many hops and link are in those ip ranges. The main purpose of doing this is to stop DDOS attack if anything happens in one of domain.



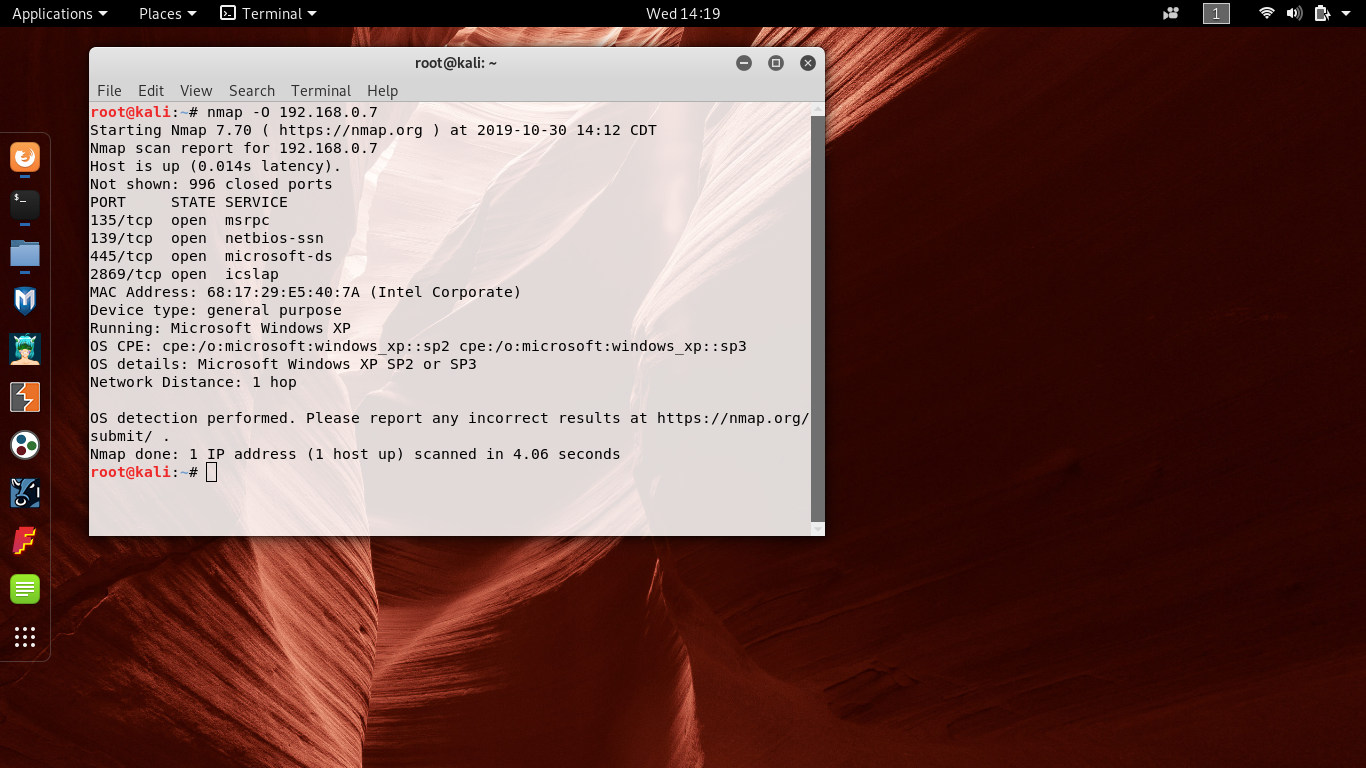
As per service it’s still uses FTP which preferably tells that they are vulnerable. Until now we performed reconnaissance and verified whether the target exists or not. We successfully verified it exists.

We mover further for scanning and enumeration.

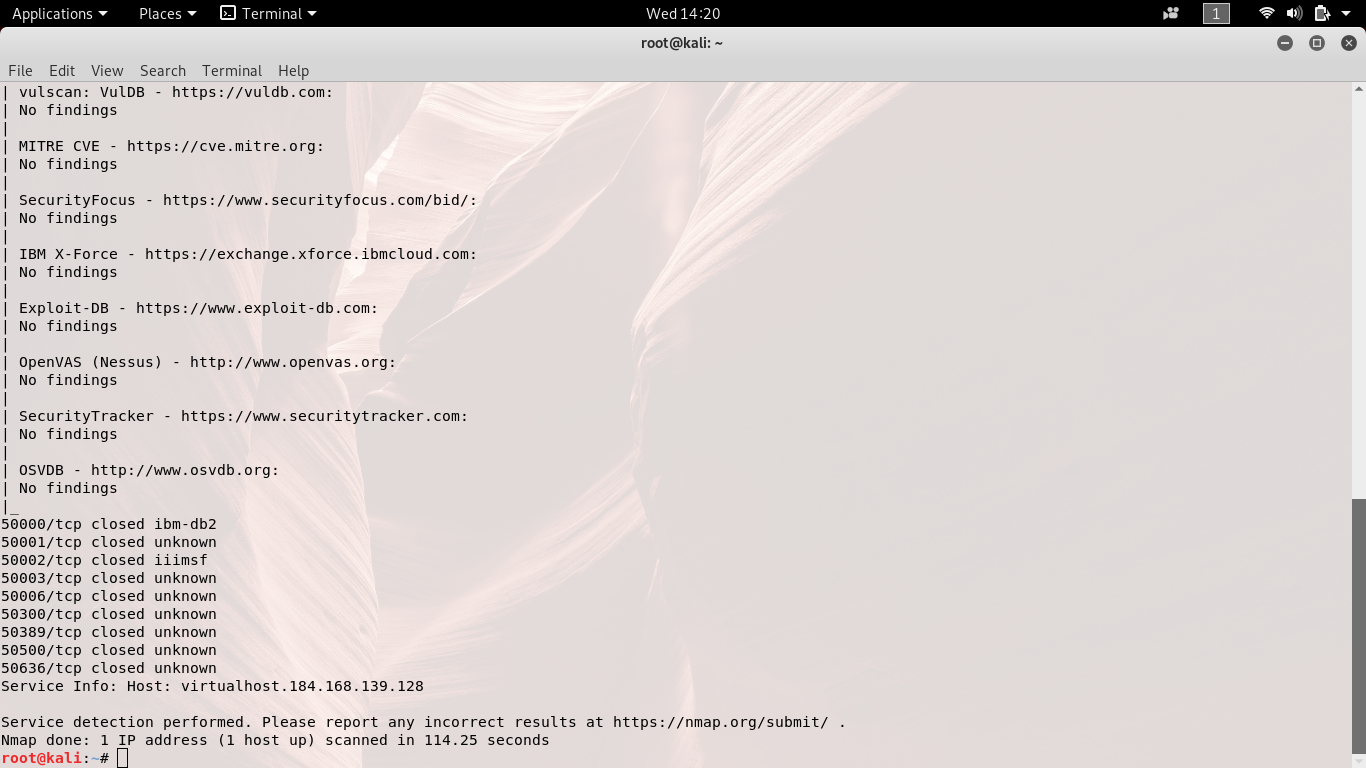
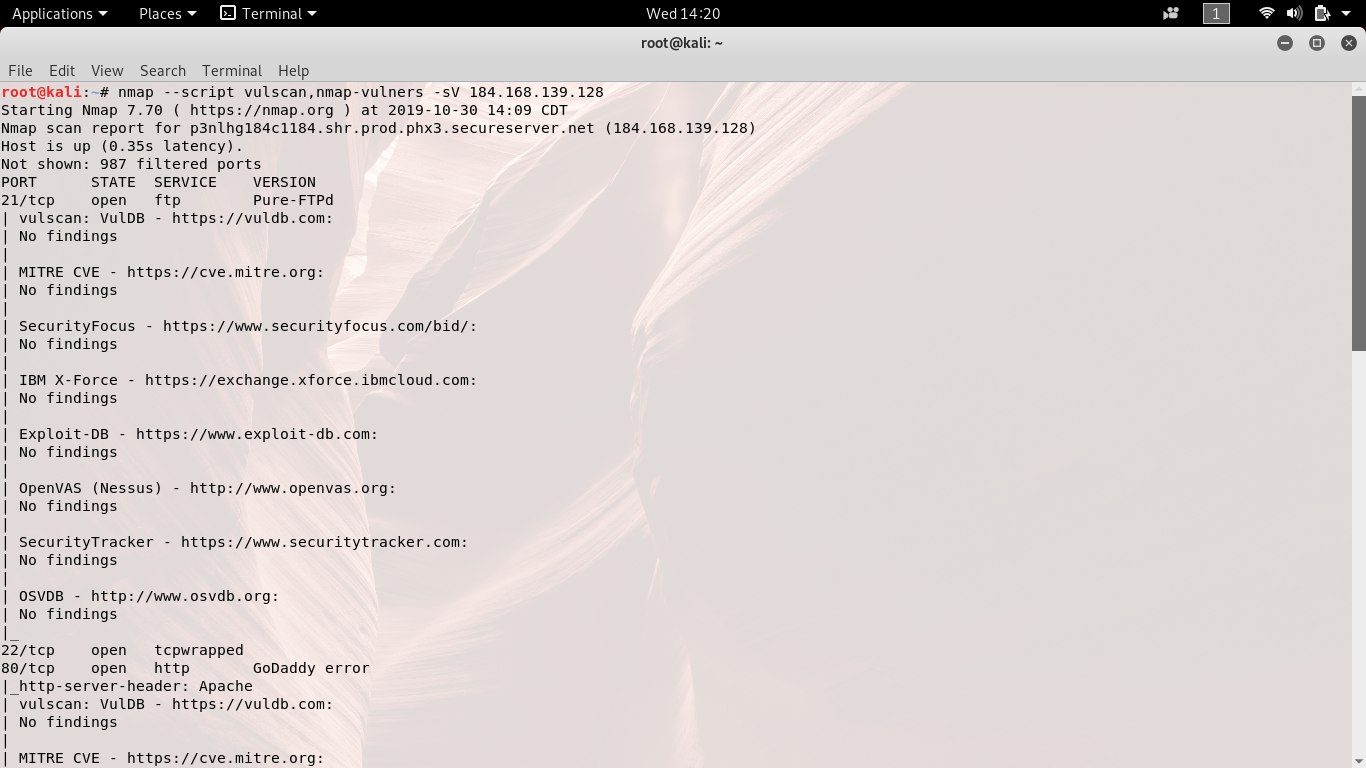
For that we will be using tools Nmap.



Here we try to guess which OS is used by target so that we can use it later for chaining.



We chained to next ip and found that 4 ports are opened which each identifies which service are running at instant.



This is most important way to determine vulnerabilty. As per result we found 0 vulnerability which is often rare case. But as we move down we see many port are closed. This is where exploit may be injected once they are opened.

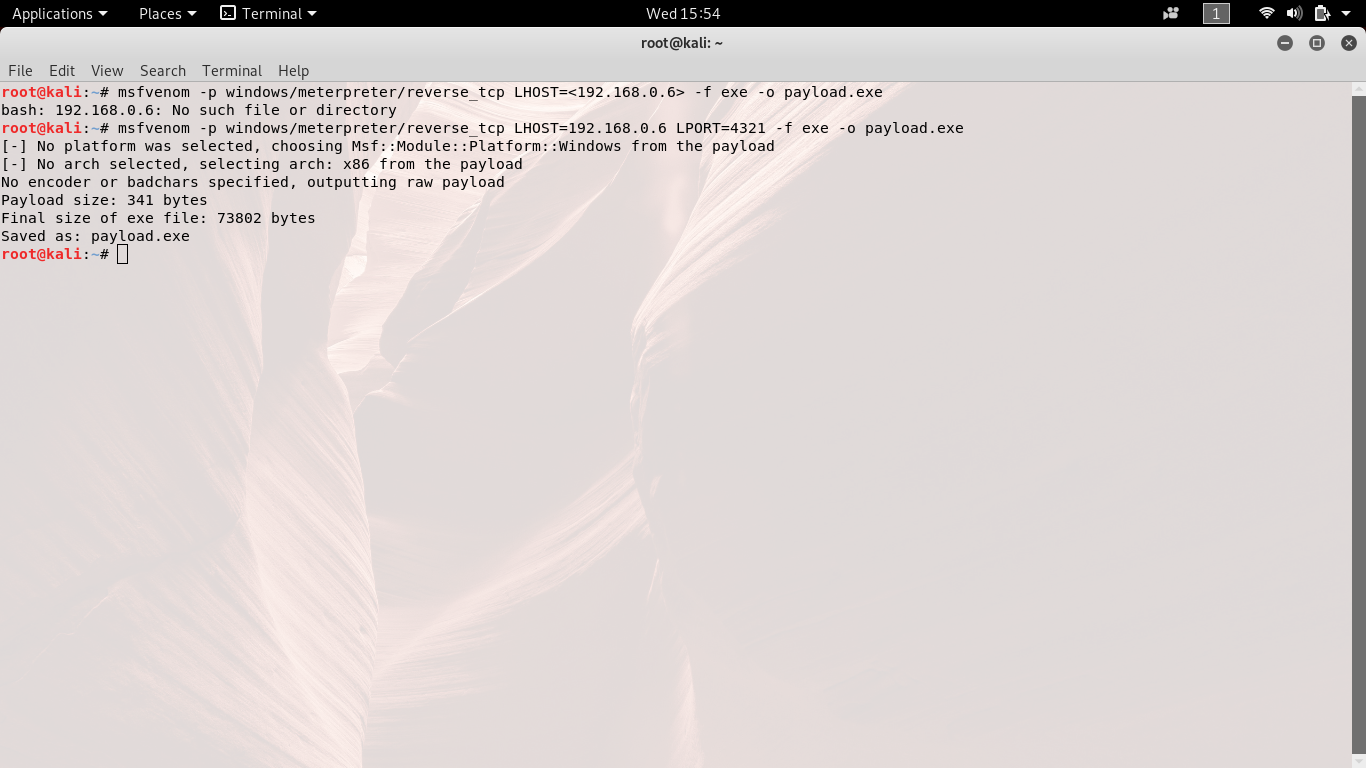


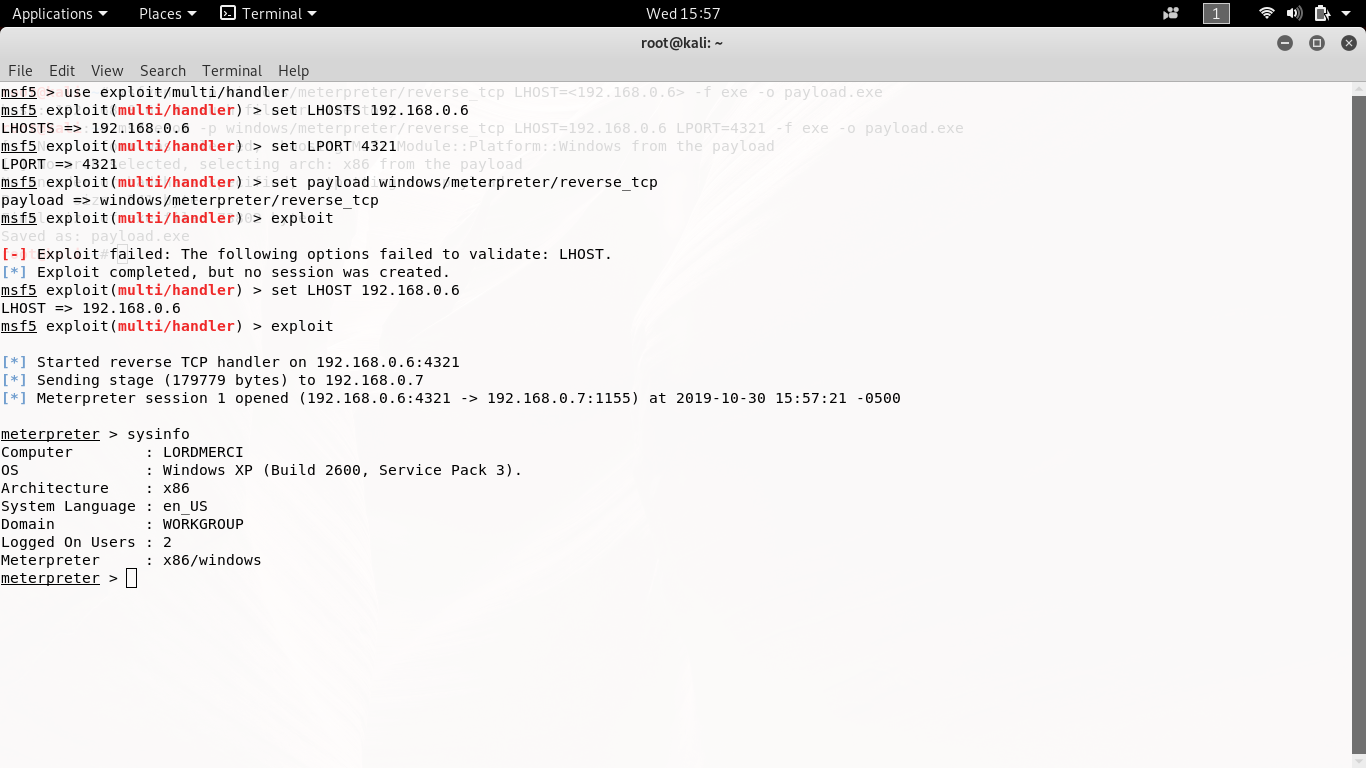
Although vulnerability is merely present but we can still see ports opened which is still risk. Among them, FTP is weaker. Http & Https indicated that there is web server present in target which later helps in web exploitation.

**ATTACK AND EXPLOITS II**

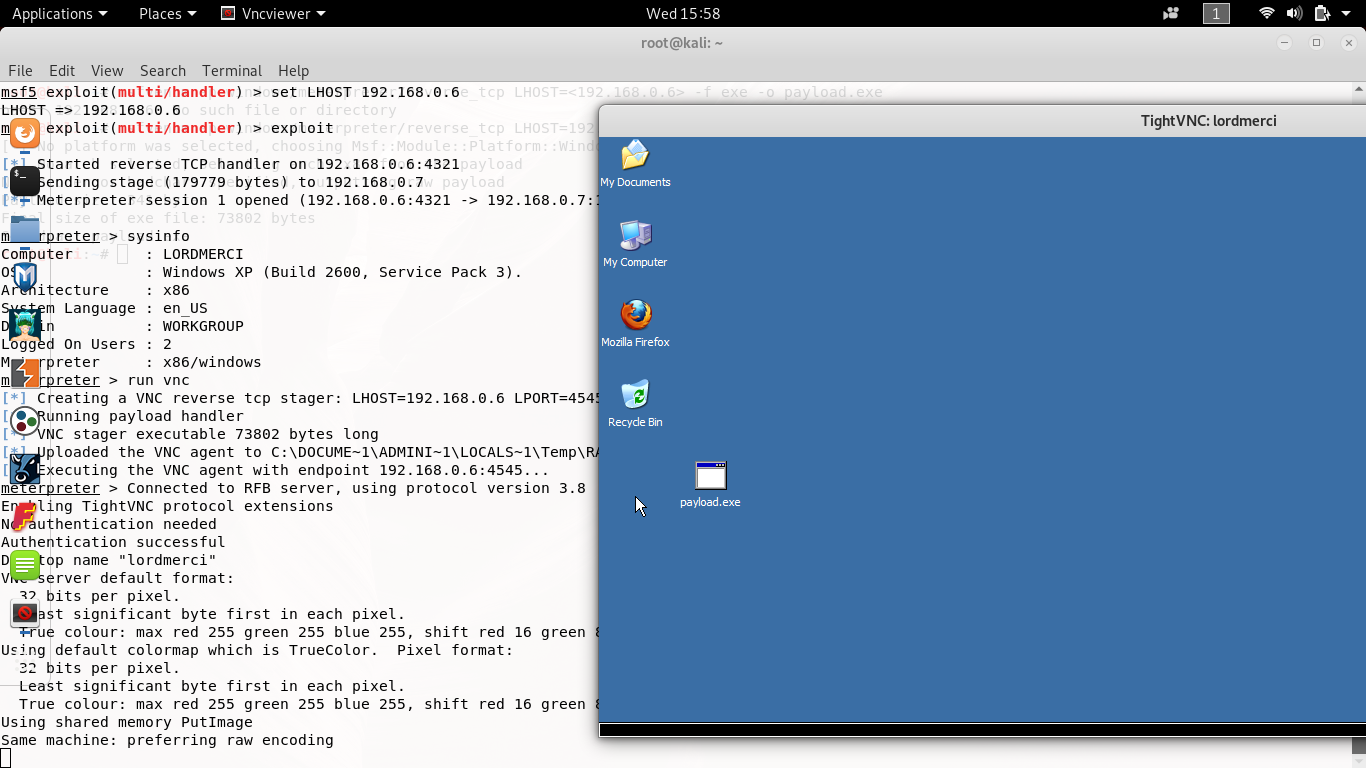
Once we determine what and where threat can be present. We come at gameplay phase where we find does this really mean target is at risk.

Let’s check and use payload





Here we create payload and inject to victim. Once victim uses we got instant sessions. After this the system is no longer controlled by user instead by tester. It is one of phase of SET (Social Engineering Toolkit).



Here is some demo what can be done once access is gained.

**Details findings**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ip address | System type | OS info | ports | | |
| Port# | protocol | Service name |
| 184.168.139.128 | client | unknown | 21 | tcp | ftp |
| 22 | tcp | tcpwrapped |
| 80 | tcp | http |
| 443 | Tcp | https |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ip address | System type | OS info | ports | | |
| Port# | protocol | Service name |
| 192.168.0.7 | chain | MS windows  XP | 135 | tcp | msrpc |
| 139 | tcp | Netbios-ssn |
| 445 | tcp | Microsoft-ds |
| 2869 | Tcp | icslap |

ANALYSIS AND REPORT

1.Unsecure service ***(Telnet)***:

Threat Level = **Medium**

Vulnerability = **Medium**

Analysis

Telnet provides access to the server for remote administration as an example. Unfortunately telnet traffic is not encrypted. Suspicious users i.e. attacker with and easy accessible sniffer can sniff the traffic, which may include sensitive data and/or administrator credentials.

Impact = **High**

Risk Rating = **Low**

Recommendation

If deemed necessary for this server to be administered remotely, utilize secure

Administration tools such as SSH or Secure remote desktop access.

2. Microsoft RPC

Threat Level = **High**

Vulnerability = **Critical**

Analysis

The remote host is running a version of Windows, which has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges. An attacker or a worm could use it to gain the control of this host.

Attack has been given in payload section.

Risk Rating **= Critical**

Recommendation

Patch the system with latest patches from MS.

3. HTTP AND HTTPS

Threat Level = **High (http)**

Vulnerability = **Critical**

Analysis

Those are network based analysis. It depends upon user and admin configuration. They can be use as portal for attacking.

Risk Rating **= Critical**

Recommendation

IDS (Intrusion Detection System) and IPS (Internet Prevention System) play important role. And use SSL (Secured Socket Layer) instead of FTP (File Transfer Protocol) service.

**BIBLOGRAPHY**

1. <https://www.DionTraining.com>
2. <http://www.atstake.com/research/advisories/2000/a101200-1.txt>
3. <http://www.securiteam.com/unixfocus/6N00S0K03U.html>.
4. <http://www.certifiedhacker.com/>