IT Sec Def Countermeasures\_PSCS\_3113\_

IT Sec Def Countermeasures\_PSCS\_3113\_

Midterm Project

Bushra Kabir

IT Sec Def Countermeasures\_PSCS\_3113

10/18/2018

Walter Pehrsson

**1**

**Foot printing**: Identifying the target, OS, and IP address

**2**

**Enumeration**

Retrieval of groups, users, information on the system.

Nessus to scan the vulnerabilities, and open ports.

**3**

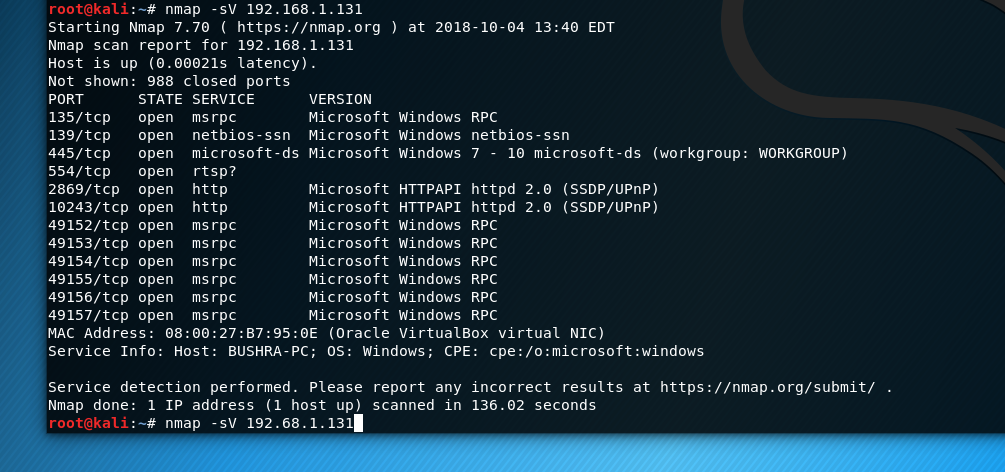
Enternal

**Attacking**

Registry, even logs, remote access,

Target: 192.168.1.131

**Nmap**



I ran the command nmap -sV to determine open ports service/version info

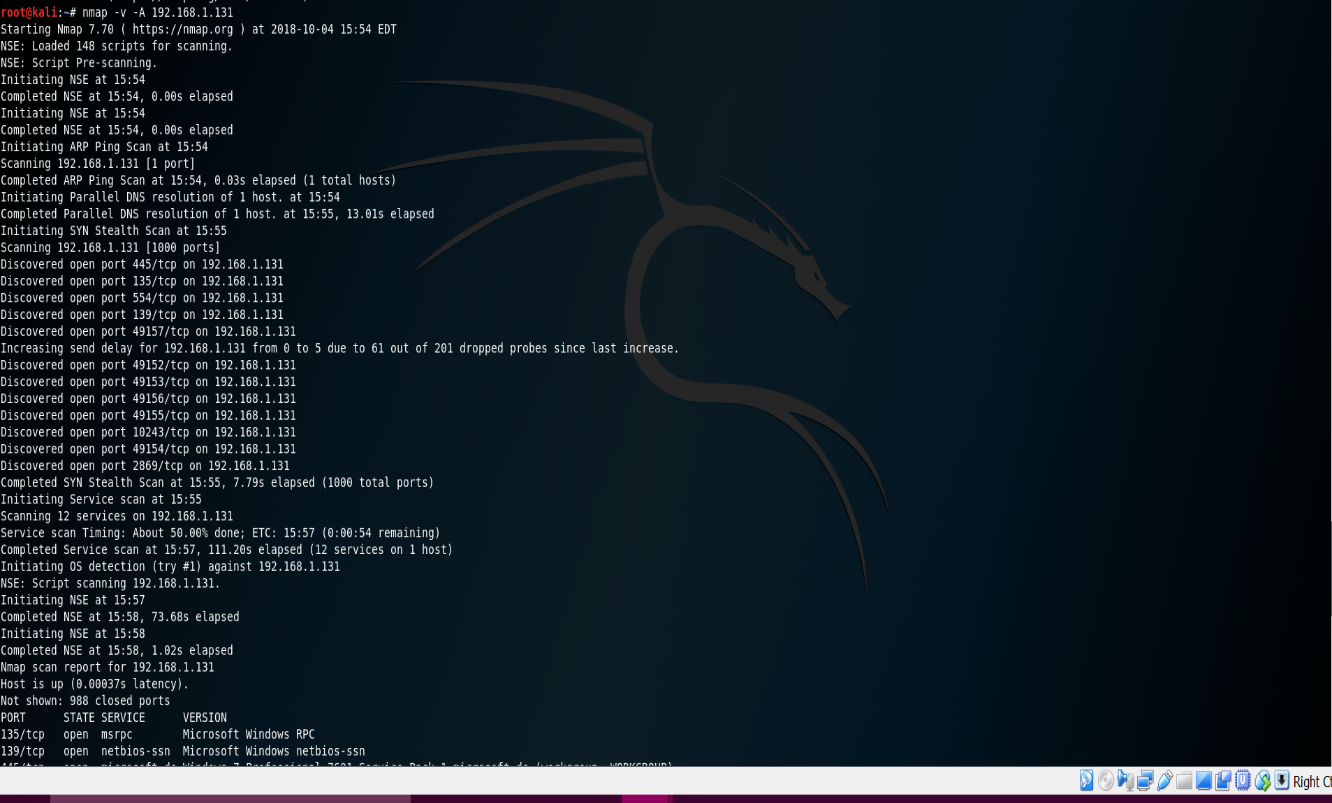
**Port open: 135/tcp**

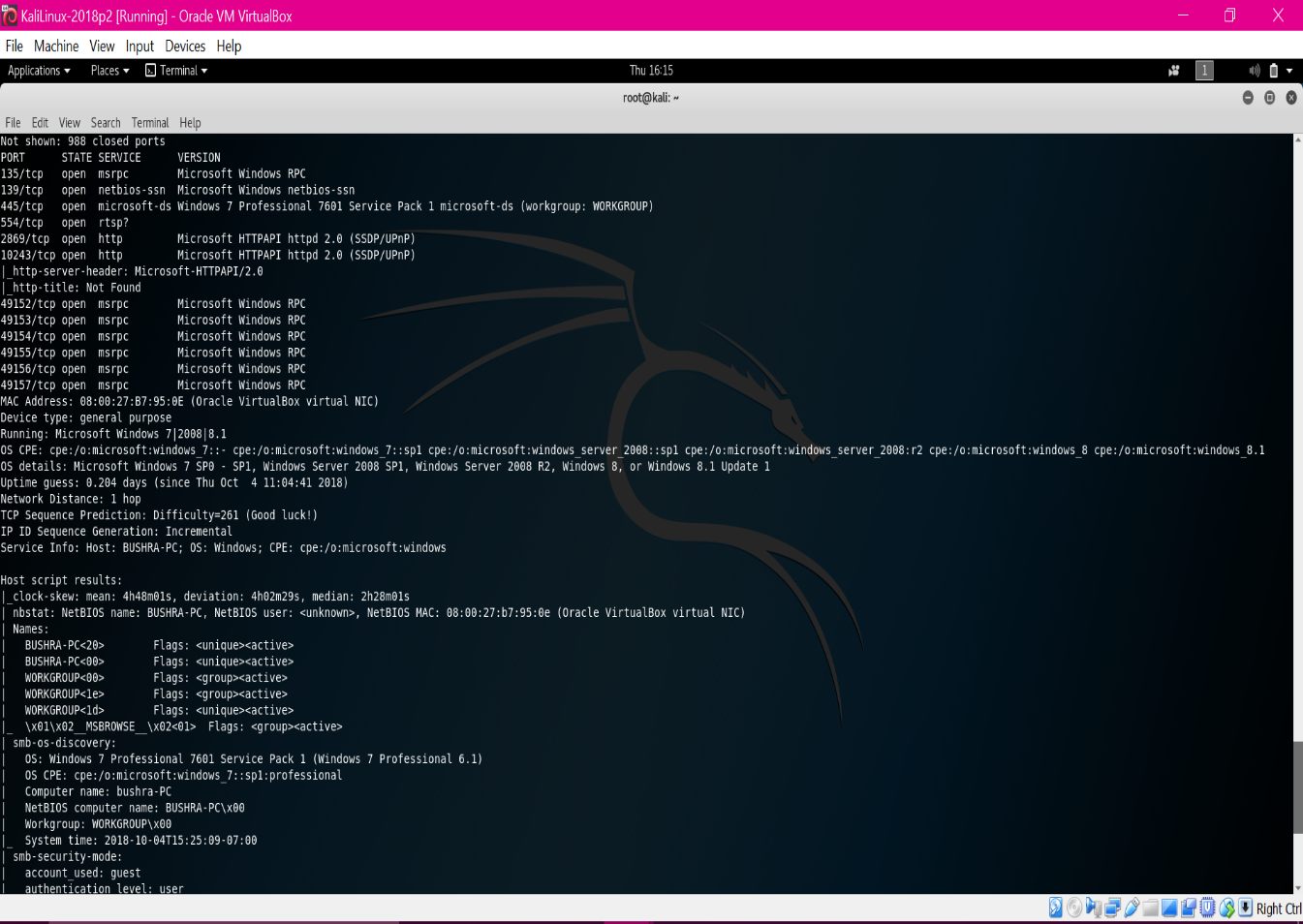
Remote Procedure Call (RPC) port 135 is utilized in client/server applications, usually on a single machine. For example, Exchange clients, which exploited messenger service, and in addition different Windows software. If you enable remote clients to get into your system through VPN, you have to open the 135 port to make the entrance to the Exchange server accessible. The RPC makes it possible for the programs on your PC to run the code on a remote PC, and infection exploits this to infect your PC.

<https://www.speedguide.net/port.php?port=135>

<https://www.drivethelife.com/windows-drivers/disable-tcp-port-135-avoid-wannacry-ransomware-windows-10-8-7-vista-xp.html>

command: nmap -v -A 192.168.1.131

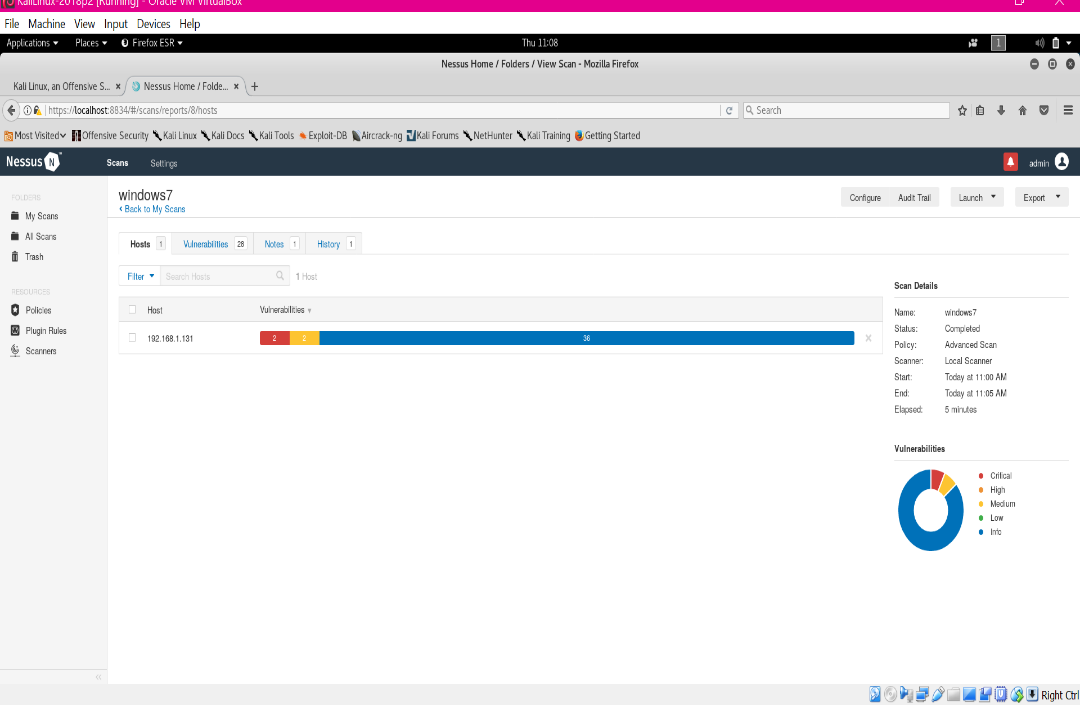


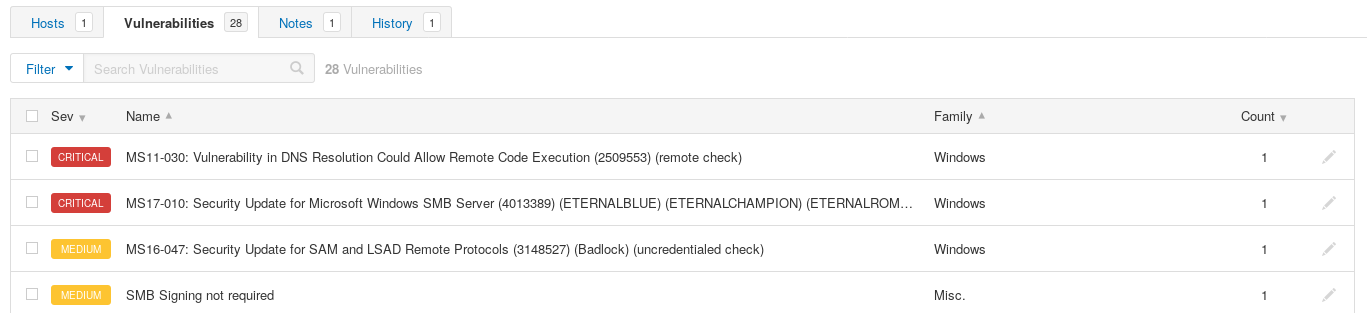


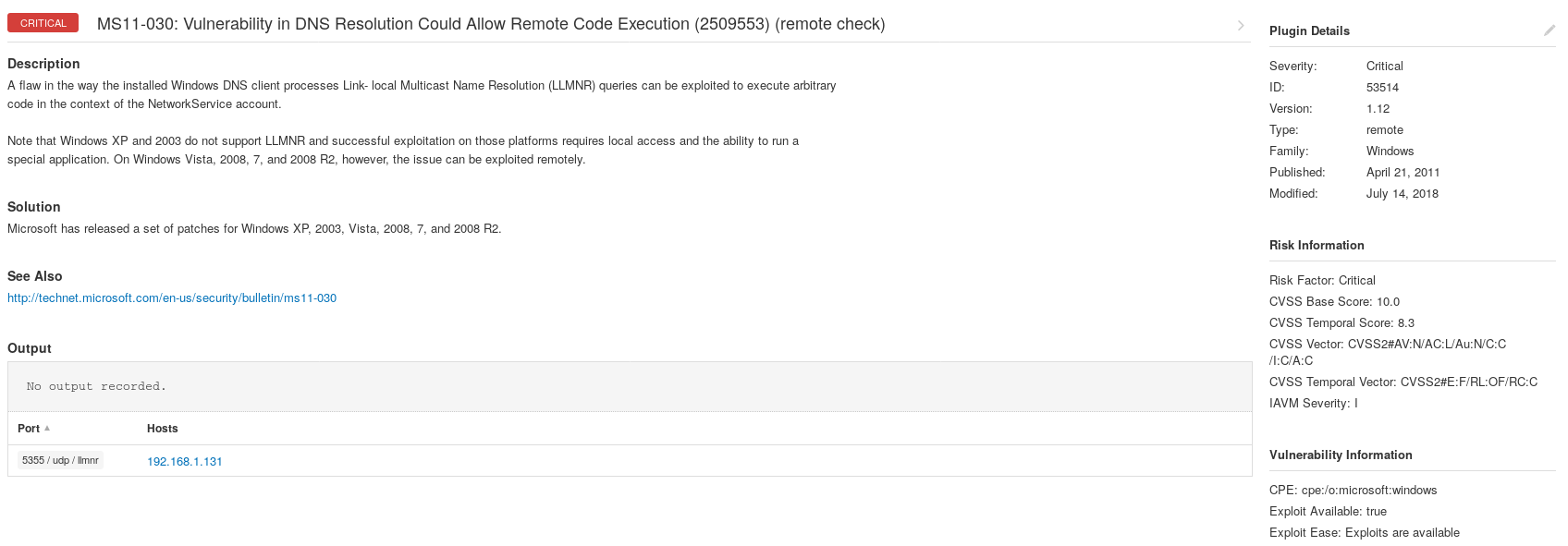


**Open Port: 139** is typically used for file/printer sharing, including directory replication with Active Directory, trusts, remote access of event logs, etc.

**Nessus**

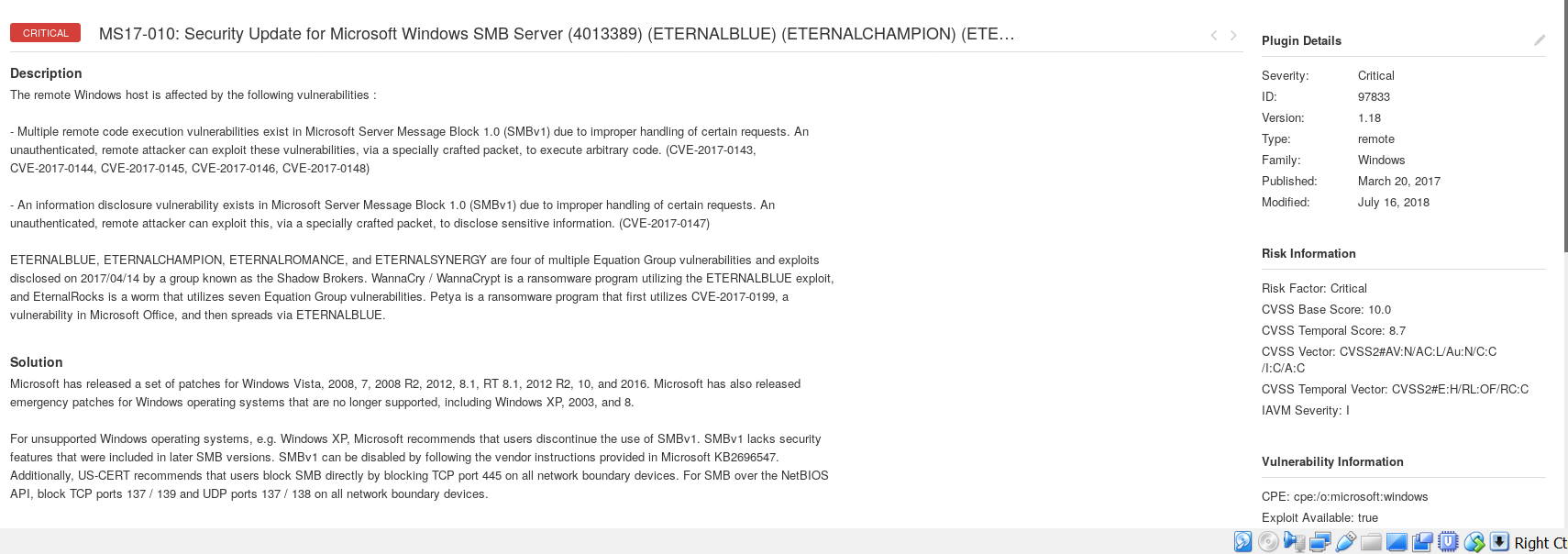
Target: 192.168.1.131



**MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)**

This security update addresses the privately reported vulnerability in Windows DNS goals. The vulnerability may allow remote code execution if the attacker accessed the system at that point made a custom program to send the Link-Local Multicast Name Resolution (LLMNR) broadcast inquiries particularly to the objective system.

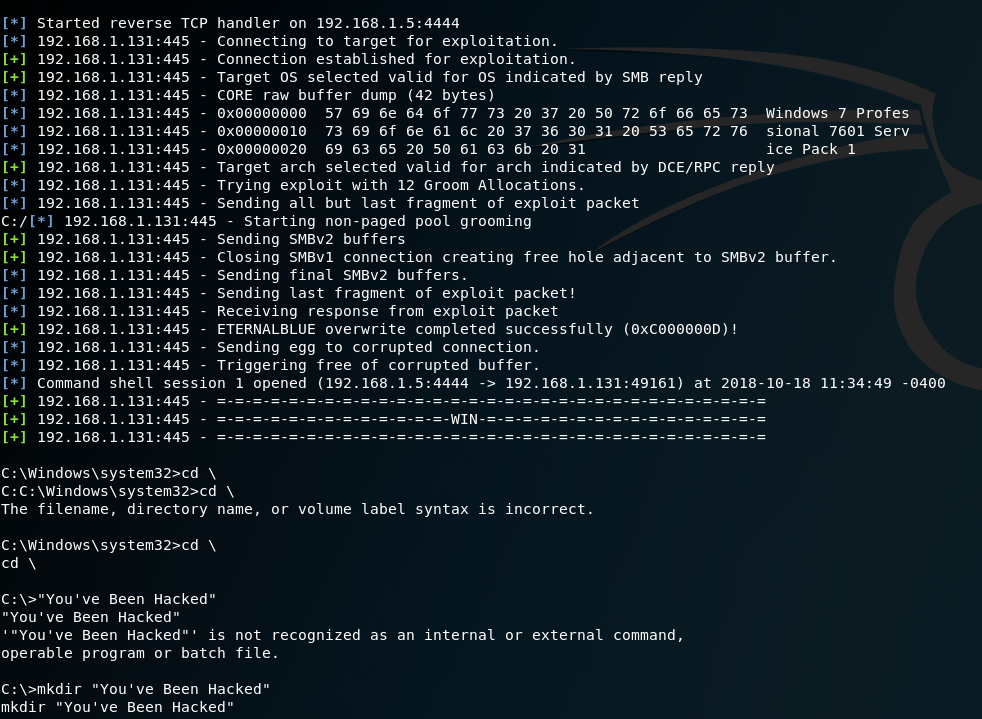
This security refresh is evaluated Critical for every single supported release of Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

**Security Update for Microsoft Windows SMB Server (4013389)**

This security update resolves vulnerabilities in Microsoft Windows. The most extreme of the vulnerabilities could permit remote code execution if an attacker sends uniquely made messages to a Microsoft Server Message Block 1.0 (SMBv1) server.The WannaCrypt ransomware is misusing one of the vulnerabilities that are a part of the MS17-010 update

**Metasploit (MS17-010)** (EternalBlue)

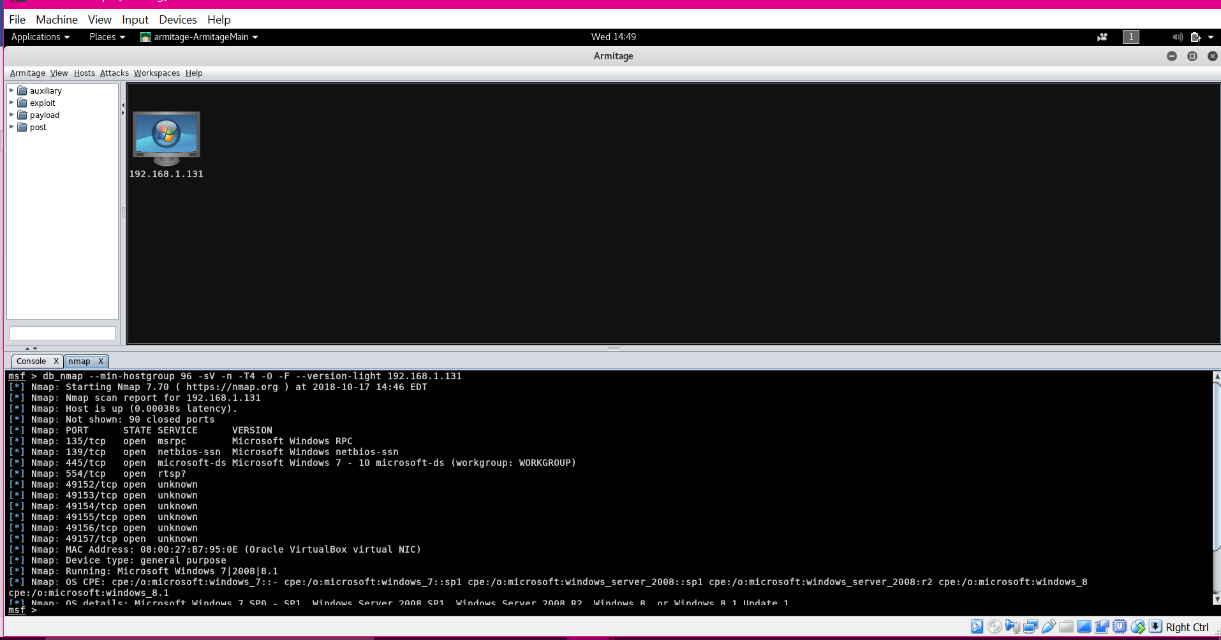




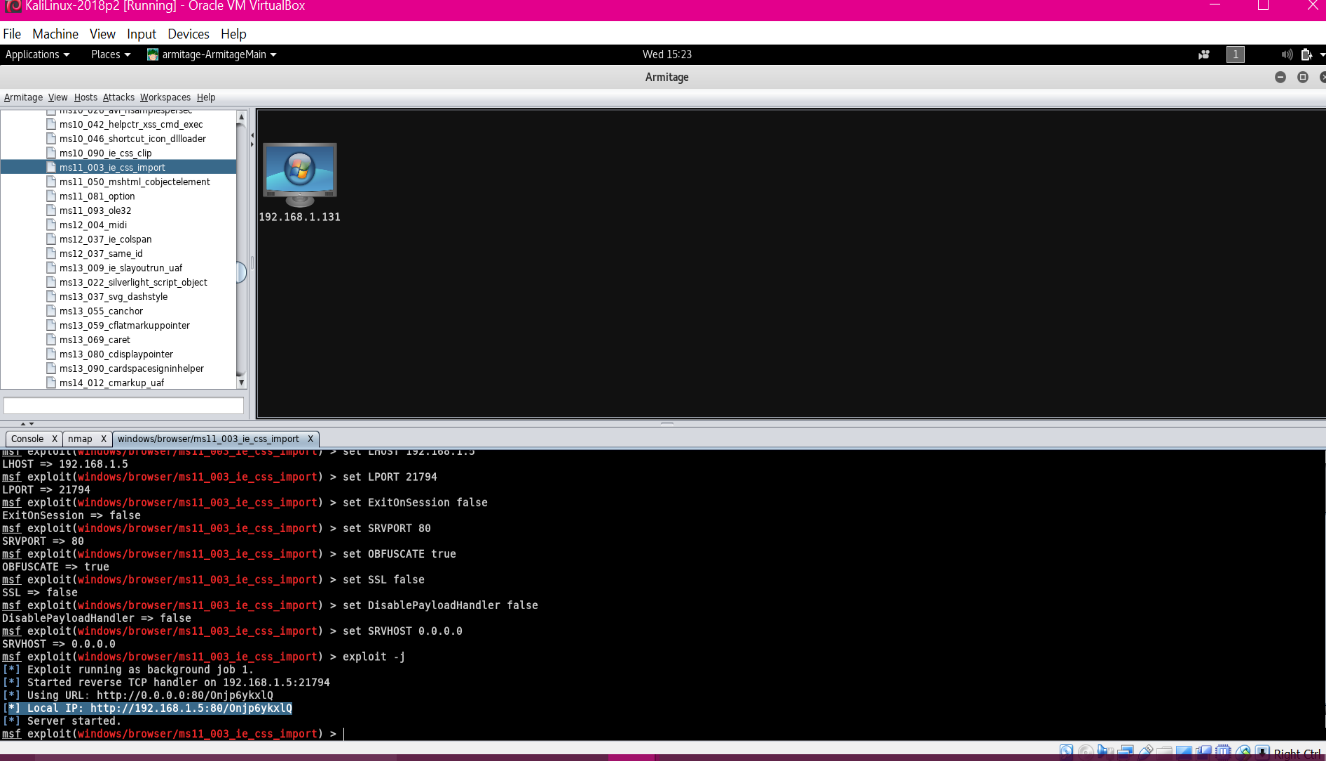
I used the vulnerability MS17-010. I used Metasploit on Kali Linux and used the command exploit/windows/smb/ms17\_010\_externalblue and hit enter. I asked the command to show me the options. The only option is set our remote host as the target machine which is 192.168.1.131. I ran the command and from there it went to the exploit. I used the standard shell. I changed myself to the root directory. I made a directory which stated you’ve been hacked. I created a file on C drive.

**Armitage**

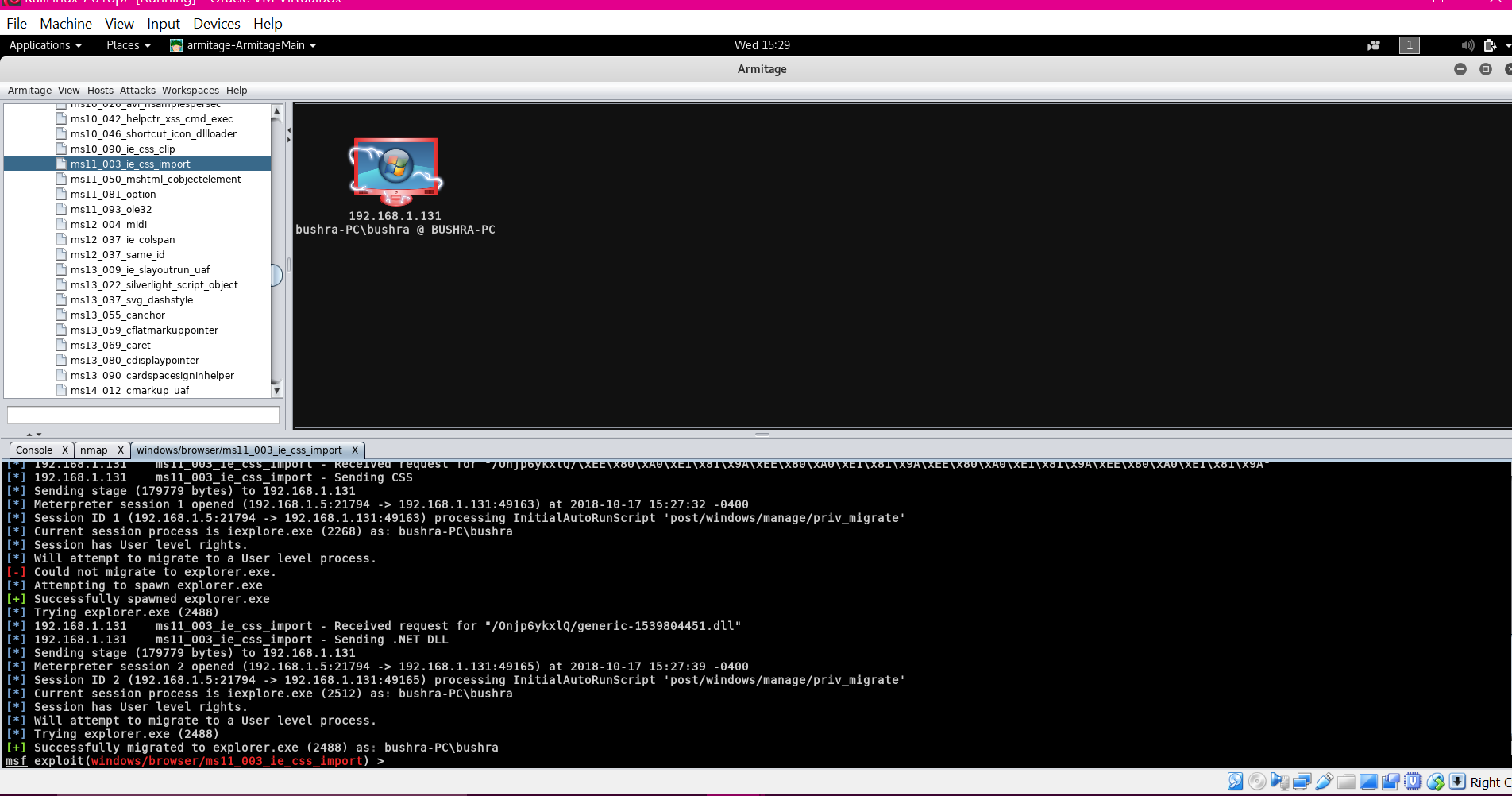
This screenshot indicate that my target machine is not compromised yet.

****

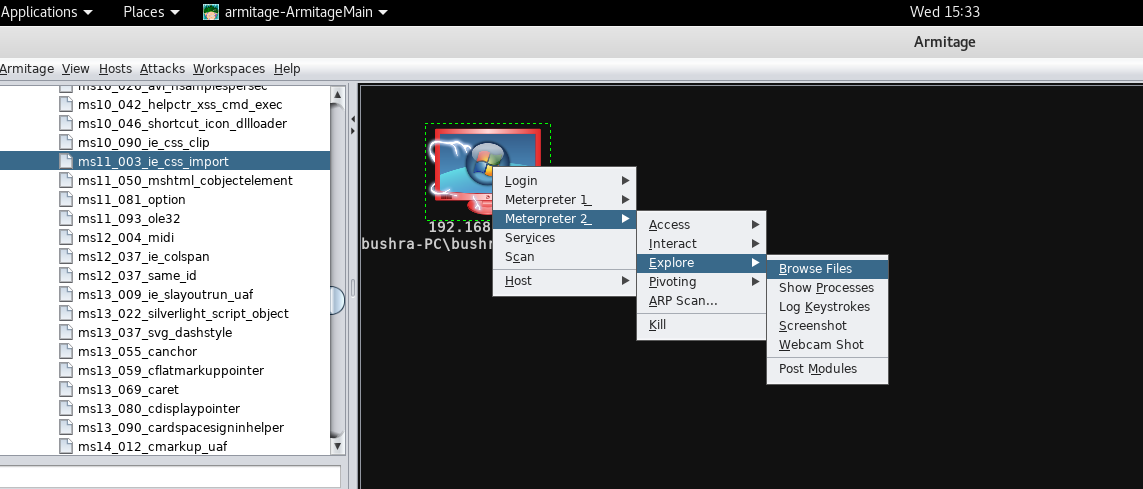
I have sent the below link to the target machine.



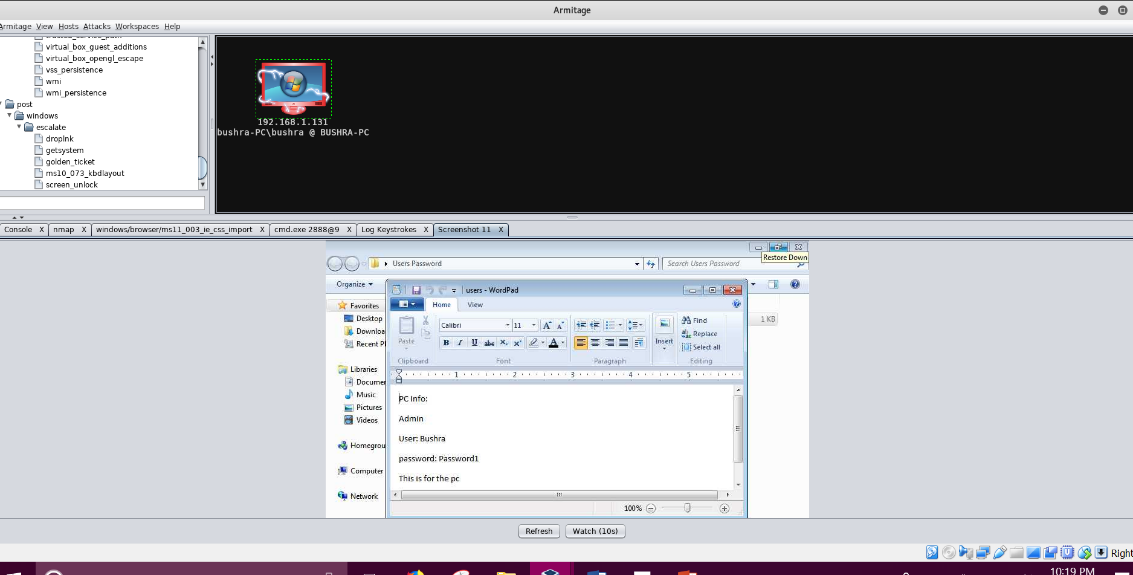
Target machine has opened the website and due to that the user machine is compromised.

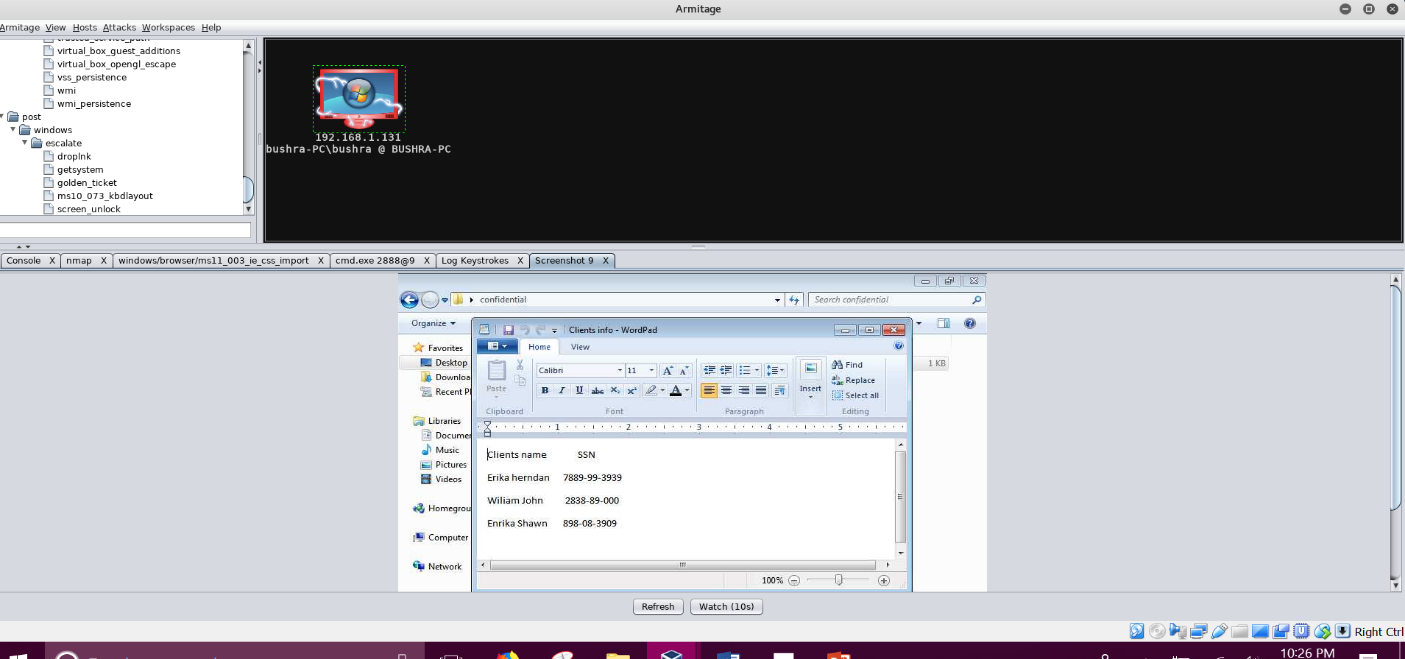


Now that I have access to the machine. I can go in and browse files, I can screenshot what the user is currently doing and also can view the log keystrokes.



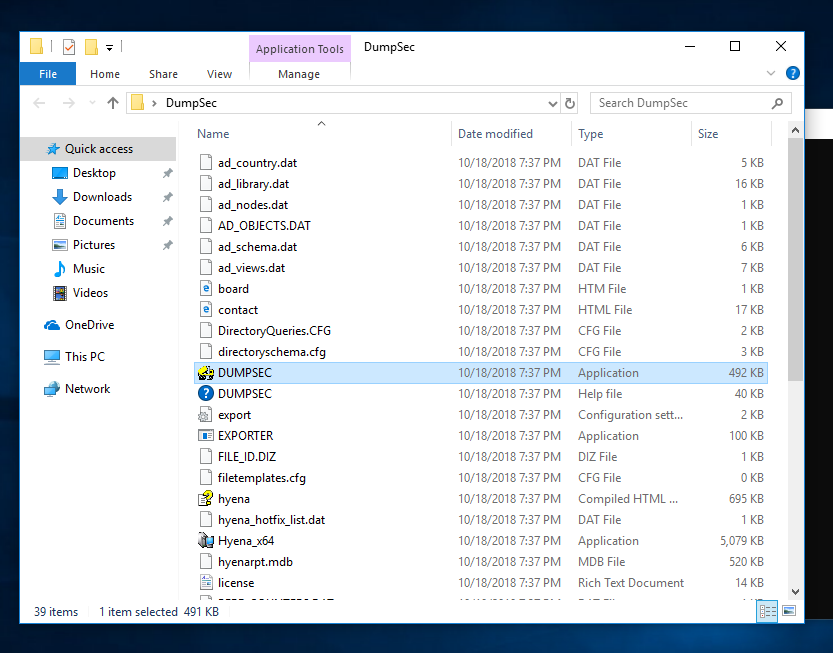
I got into the target desktop and as you can some of client information was open. Here is the screenshot of target user name and password.

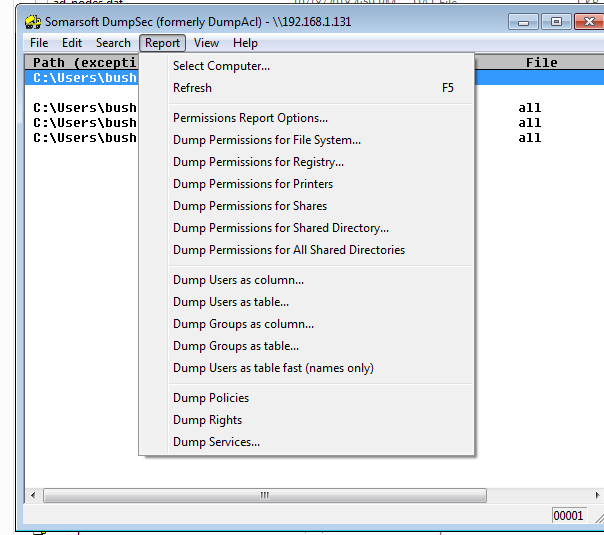


. I was able to take a

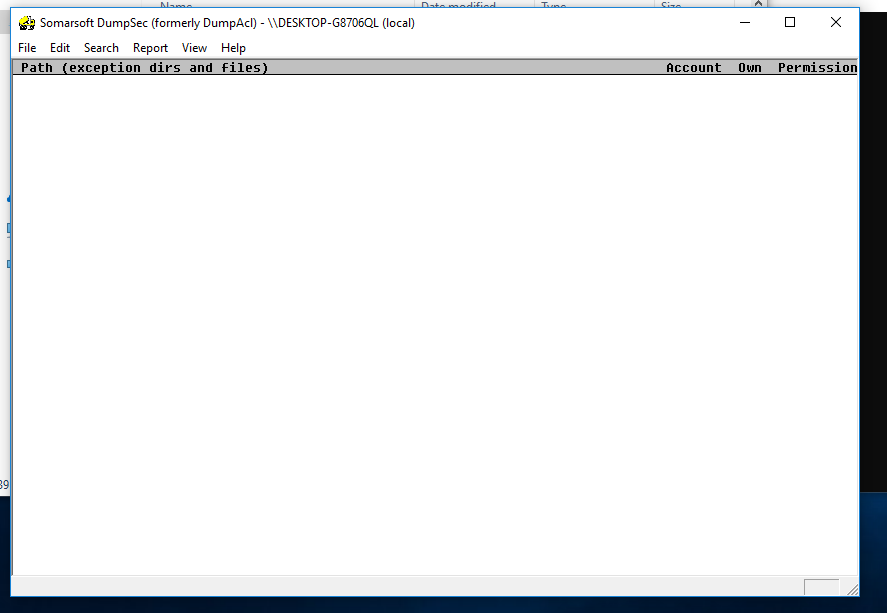
screenshot of the target machine. I was able to see the open file of client which include their names and SSN.

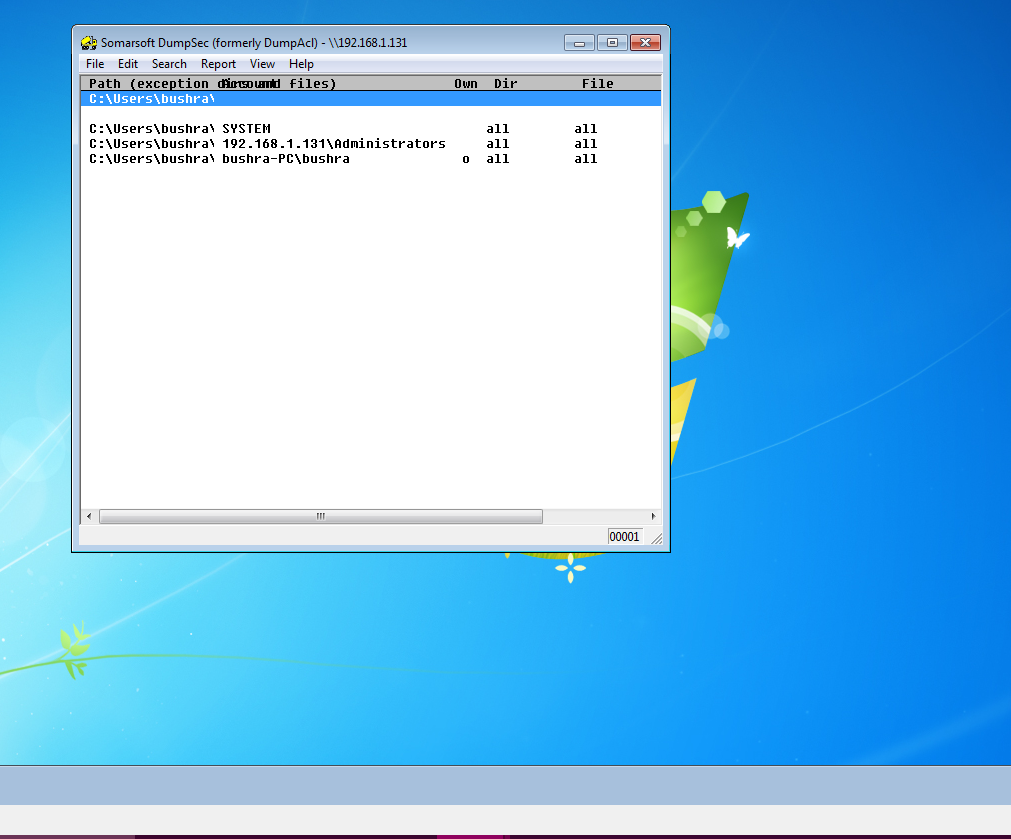
**DumpSec**

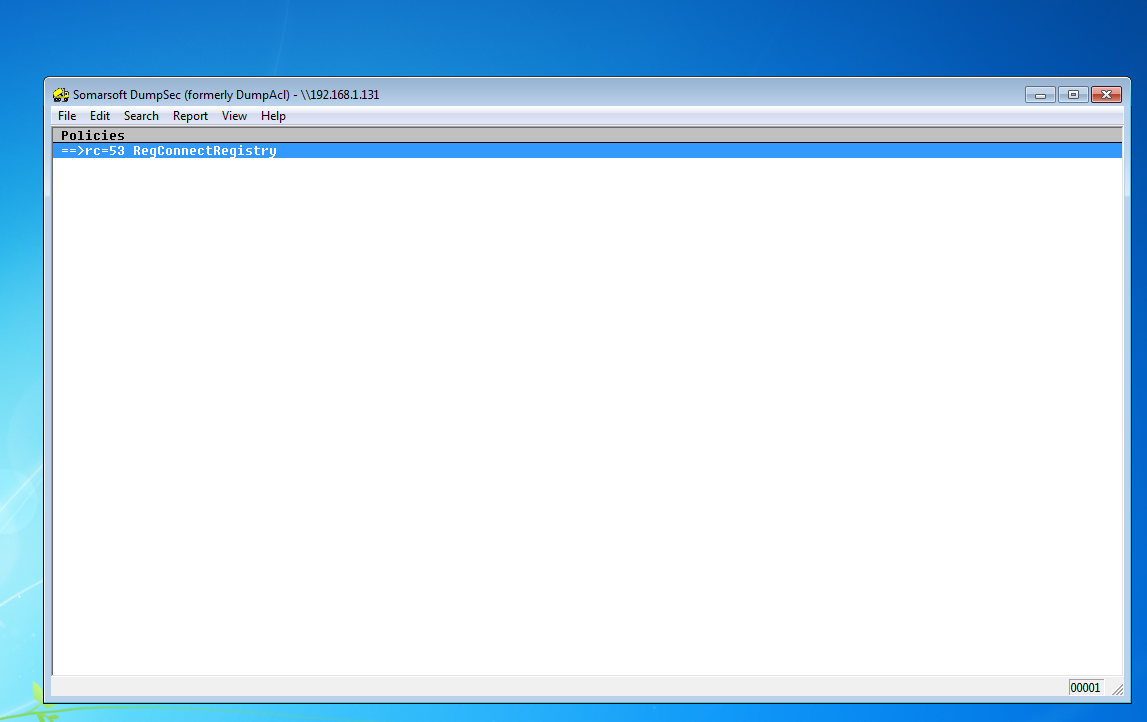
DumpSec is a security auditing program. I installed DumpSec on windows 10 and my target machine was windows 7.

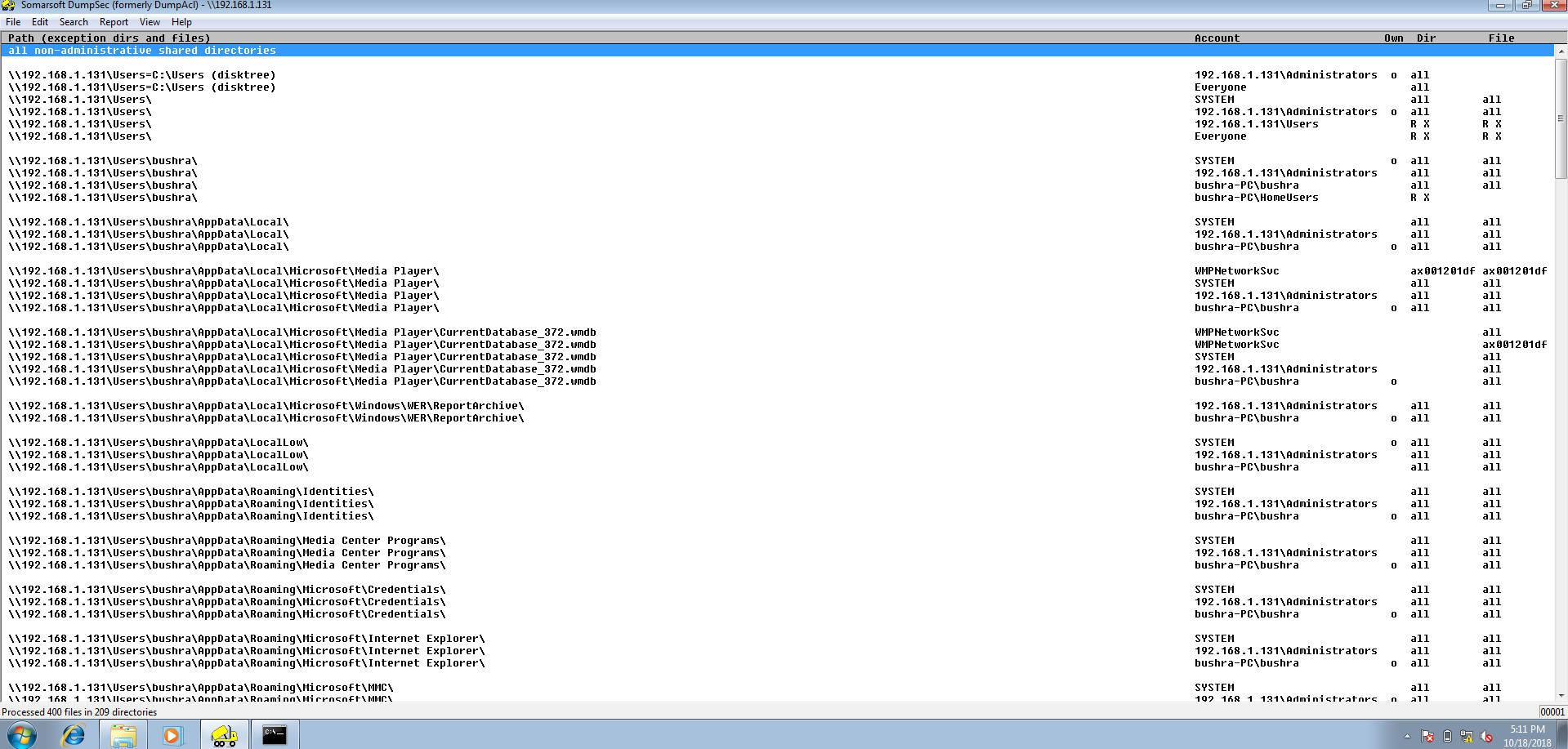


I am able to check the registry of the victim target.









I have gained a lot of knowledge by doing this project. I have learned that how small vulnerabilities can make your system compromised. For instance, how users just ignore the warning which can cause a major issue. For my target machine I was using Windows 7, when I ran Nmap scan, I was shocked to see so many ports open. I did wonder that in real life how many users are using Windows 7 and they didn’t get the updated patches. Furthermore, I scanned the vulnerabilities by using Nessus, and found few critical ones. It was amazing to see what Kali Linux can do. Kali Linux have some amazing tools which is good for penetrating testing. When I used Armitage tool and exploit my target machine, I found out a lot of things. I was able to get into the system, I was able to take screenshot of what the user is doing. Also, I was able to save keystrokes, and look through the files. The user had no idea that the system was compromised, because there is nothing suspicious going on. On the same time, it was scary to know what these vulnerabilities can do to your system. Basically, your whole information is out there, and you have no idea. Additionally, I used Metasploit to exploit MS17-010 vulnerability. I did get into the system, and I have able to create a folder inside the system. I created a folder named Hacker inside windows 7. I have learned that it is important to update your software and have a strong password which is not easily to crack. My last tool that I used was DumpSec. It is used for security auditing program. I got into the target machine and I was able to check the registry. Also, for me to understand the tools better I had to do a lot of research. Finally, my experience was great learning about the tools and finding out which tools can exploit the vulnerabilities. Overall, I enjoyed learning and exploring what is out there.

**Citations**

SpeedGuide, U. (2017, September 02). Port 135 (tcp/udp). Retrieved October 12, 2018, from <https://www.speedguide.net/port.php?port=135>

Shaw, B. (2018, September 10). Disable TCP Port 135 and Avoid WannaCry Ransomware on Windows 10, 8.1, 8, 7, Vista, XP. Retrieved October 4, 2018, from https://www.drivethelife.com/windows-drivers/disable-tcp-port-135-avoid-wannacry-ransomware-windows-10-8-7-vista-xp.html

B. (2015, March 13). Microsoft Security Bulletin MS11-030 - Critical. Retrieved October 11, 2018, from https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-030

B. (2017, March 14). Microsoft Security Bulletin MS17-010 - Critical. Retrieved October 10, 2018, from <https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010#security-update-for-microsoft-windows-smb-server-4013389>

Dion, J. (2017, July 05). EternalBlue Exploit Against Windows 7 (MS17-010). Retrieved October 18, 2018, from https://www.youtube.com/watch?v=\_yOkfS21hbw

Sploit, H. (2018, April 12). Armitage Kali Linux Tutorial - Scanning & Exploitation. Retrieved October 18, 2018, from https://www.youtube.com/watch?v=JALmoY4LuT8

Armitage. (2014, February 15). Retrieved October 18, 2018, from <https://tools.kali.org/exploitation-tools/armitage>

Jetwee, L. J. (2016, March 16). Kali Linux - Armitage (Nmap & Metasploit). Retrieved October 17, 2018, from https://www.youtube.com/watch?v=A1qR8lwpW2E

SomarSoft Utilities. (n.d.). Retrieved October 18, 2018, from https://systemtools.com/somarsoft/?somarsoft.com