The George Washington University

Attacking Windows 7

By: Troy Cabral

Course: PSCS3113

Due: 10-18-18

Professor Walter Pehrsson

Contents

Project Summary

Machine Configurations

All machines will be installed via Virtua Box. The target machine will be a windows 7 machine configured with an IP address of 192.168.1.100/24. The Windows firewall will be turned off and no updates performed. The main attack machine will be Kali Linux, with Windows 10 being used for one tool, Dumpsec. All machines will be disconnected for internet and will communicate via a virtual Local Area Network.

Tools Used: DumpSec

DumpSec was downloaded from SystemTools.com and installed on a Windows 10 machine. DumpSec can collect detailed information about user accounts as well as "permissions (DACLS) and audit settings (SACLs) for the file system, registry, printers and shares" (SystemTools, n.d.). In Screen Shot 1-1 a scan for user information is performed, showing a total of 5 accounts, two of which are administrator account. It also shows that the administrator account TC doesn't require a password. Having no password requirement for an admin account is a huge security vulnerability and if found in a real world scenario would need to be fixed immediately.

Tools Used: Nessus

Nessus is one of many vulnerability scanners available online. Using Nessus as an enumeration tool will give attackers knowledge of what exploits they can execute. Screen Shot 2-1 shows the results of the vulnerability scan on the target machine. Four total vulnerabilities

were found, two critical and two medium. Clicking on each vulnerability will bring up a section that gives details, solutions, and even links out to other resources like CVE.Mite.org (common vulnerabilities and exposures). Screen Shots 2-2 through 2-5 show the vulnerabilities found in an unpatched Windows 7 machine. Screen Shot 2-6 shows that after patching, only one medium vulnerability is left, which is SMB signing is not required.

Tools Used: NMAP

NMAP is another enumeration tool, but unlike Nessus, it uses the command line interface (CLI). With this tool information like open TCP/UDP ports, IP protocols in use, and Operating system details can be identified (pictures 3-1 through 3-4). Information gathered with NMAP can be combined with the information from Nessus to get a better idea of not only the weaknesses of an attack target, but also of the network layout.

Tools Used: BeEF

BeEF stands for Browser Exploitation Framework and can send commands to someone's browser to be executed (Occupytheweb, 2015). It requires some work before the attack can be sent to the targets browser first though. The first step would be for someone to visit a website that has been infected, and if they are able to run a file called "Hook.js" from the infected website, their browser will become hooked (Occupytheweb, 2015). Screen shot 4-1 shows a demo of a browser becoming hooked. The demo is merely a way to practice using BeEF without having to infect a website and send commands to an unsuspecting victim. Once a browser has become hooked, the IP and details of the victim will populate in the BeEF application (screen shot 4-2). From here an attacker can gather information about the browsers vulnerabilities and

can send commands for the browser to execute. Screen Shot 4-3 shows the execution of a phishing attack. While the webpage resembles what an gmail email login might look like, it is completely fake. If someone were to fall for this type of phishing and enter their username and password for their gmail account, that information would be passed back to the attacker to utilize.

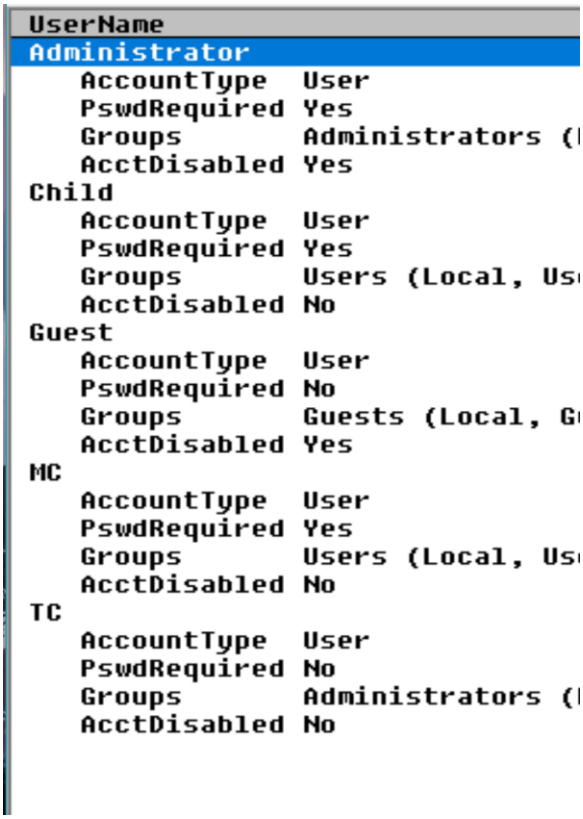
Tools Used: Metasploit

Metasploit is a powerful tool distributed by Rapid7 that allows a user to find vulnerabilities and exploit them (Metasploit, n.d.). In this example, the exploit EternalBlue was executed. Screen shot 2-3 also shows that Nessus picked up that the target machine might be vulnerable to this type of attack. Screen shot 5-1 shows how easy it is to set up and execute once it is known that the target machine is vulnerable. All that needs to be done is the selection of the exploit, setting target IP, and running the exploit. Afterwards the attacker would have access to the CLI on the target's machine. Microsoft has release a patch for this vulnerability, so only outdated systems are vulnerable.

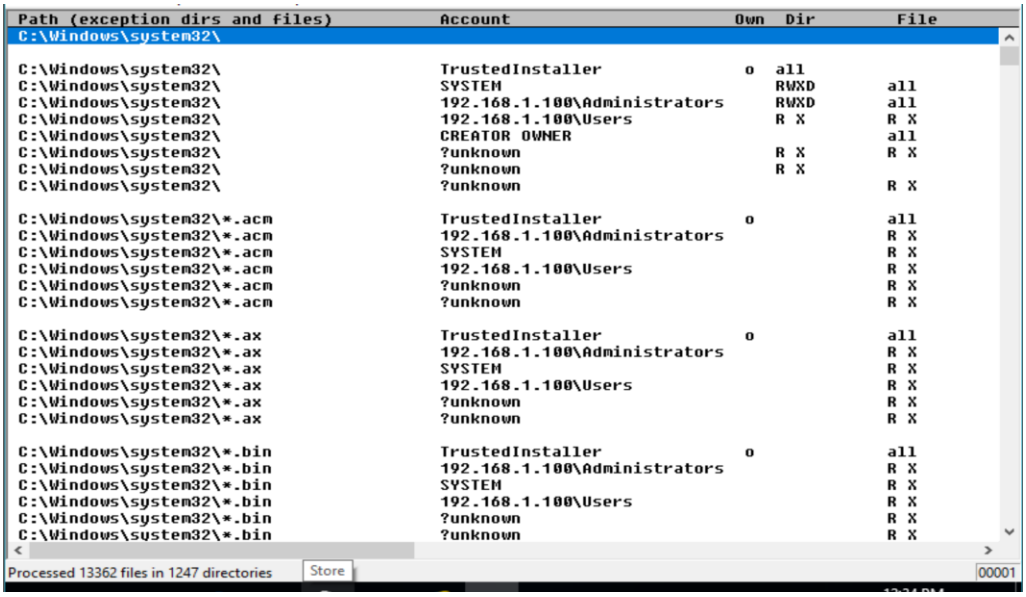
Appendix

Screen Shots: Dumpsec

1-1: Dump of Username, Account type, if a password is required, group, and if the account is active/disabled



1-2: Dump of Windows 7 File System

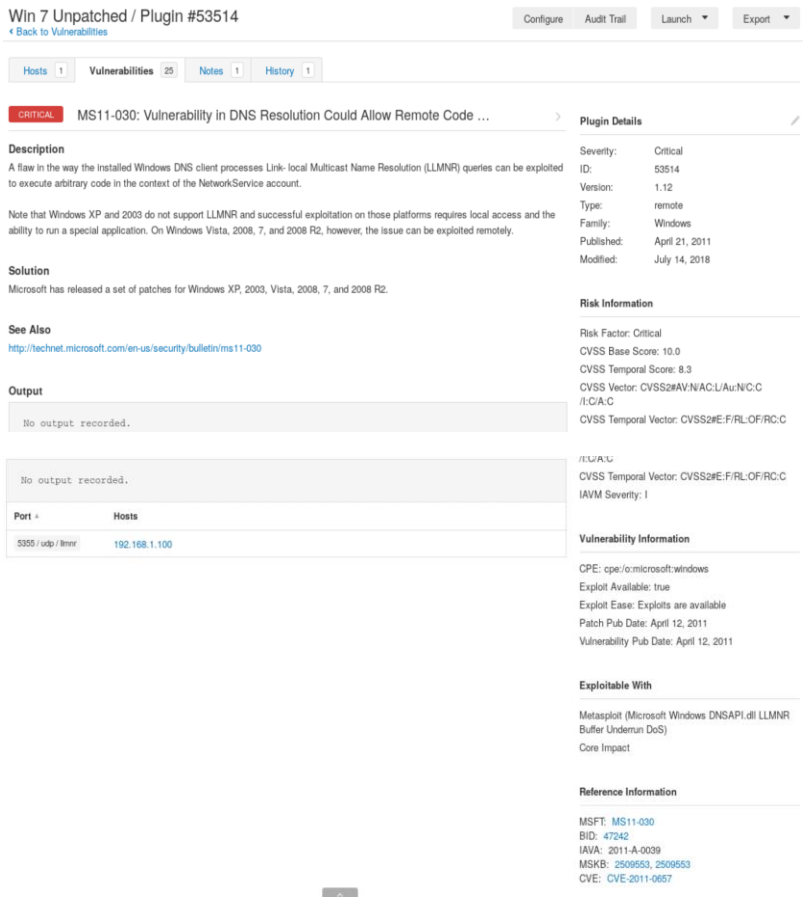


Screen Shots: Nessus

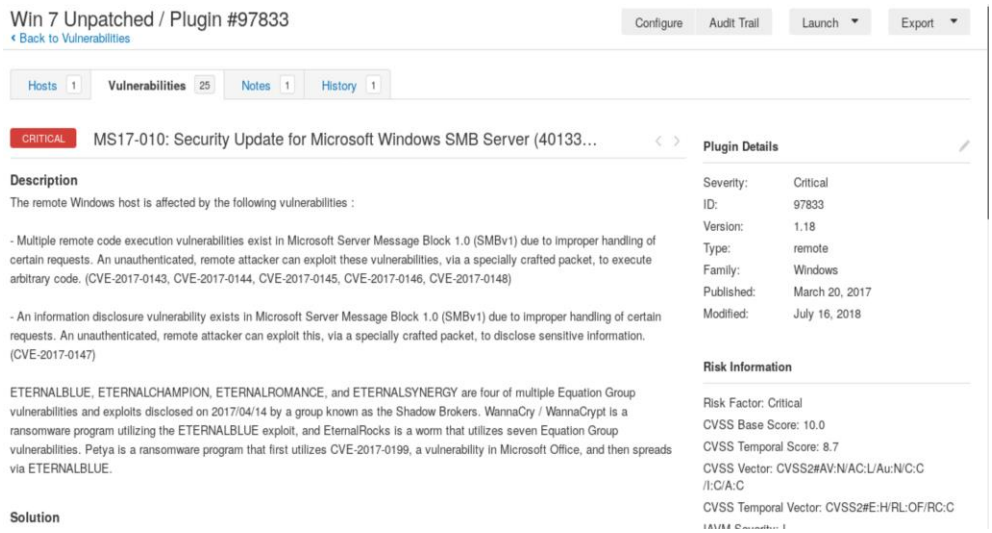
2-1: Vulnerability Scan

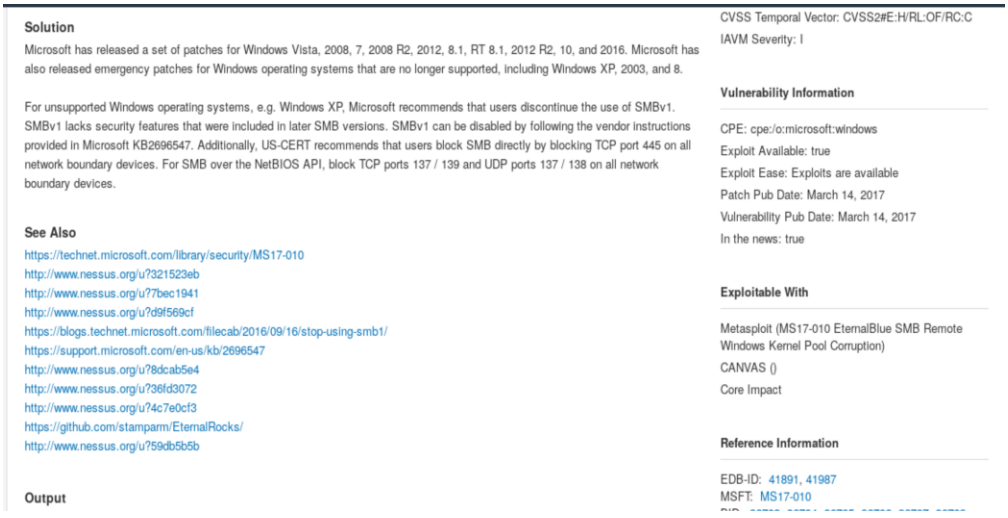
Sev	Name	Family	Count
CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allo...	Windows	1
CRITICAL	MS17-010: Security Update for Microsoft Windows S...	Windows	1
MEDIUM	MS16-047: Security Update for SAM and LSAD Remo...	Windows	1
MEDIUM	SMB Signing not required	Misc.	1
INFO	DCE Services Enumeration	Windows	8
INFO	Nessus SYN scanner	Port scanners	3
INFO	Microsoft Windows SMB Service Detection	Windows	2
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1

2-2: Vulnerability MS11-030

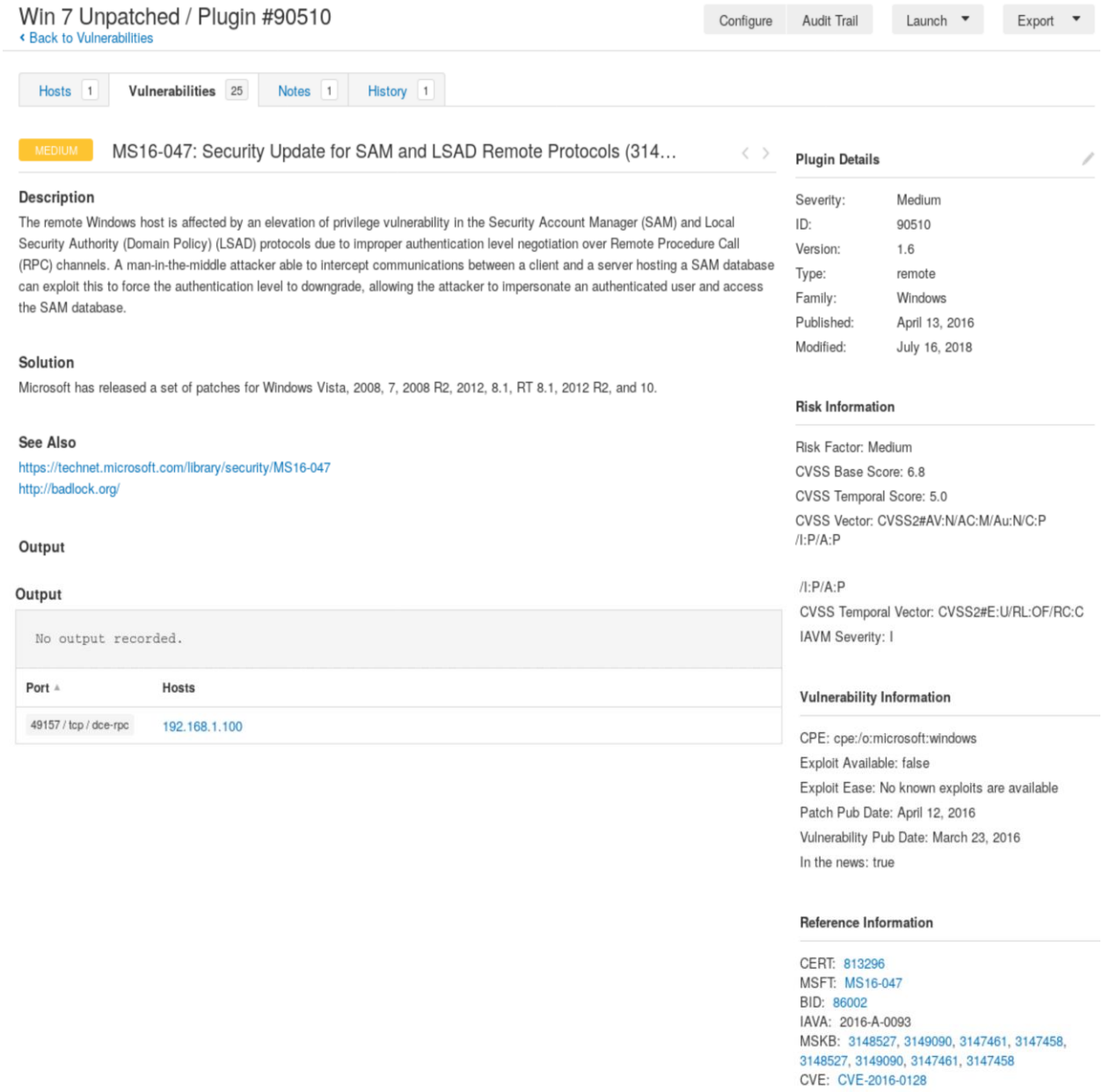


2-3: Vulnerability MS17-010

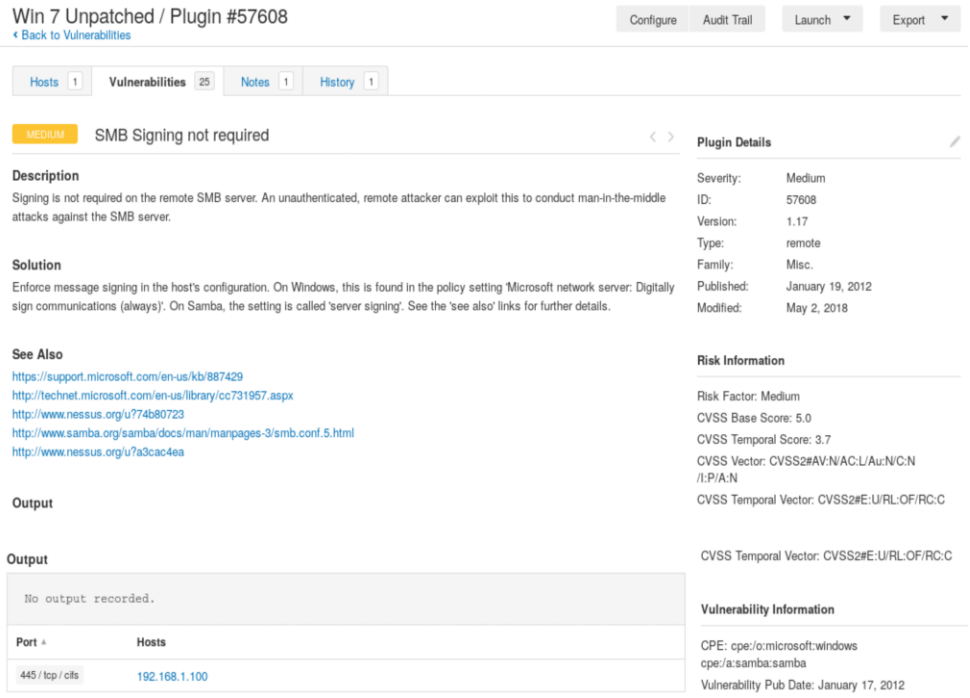




2-4: Vulnerability MS16-047



2-5: Vulnerability SMB signing not required

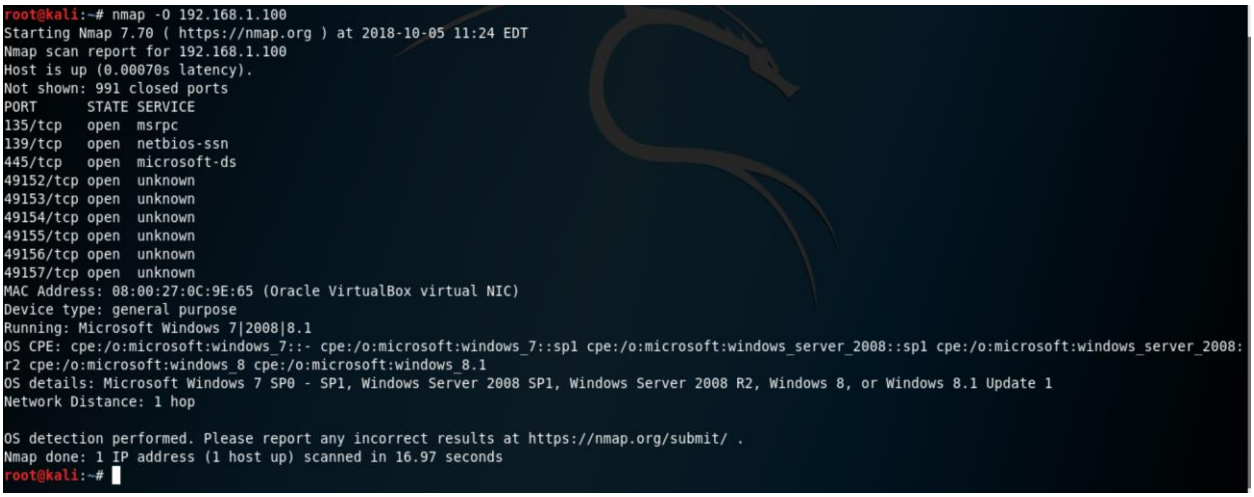


2-6 Vulnerability scan after running all Windows 7 updates

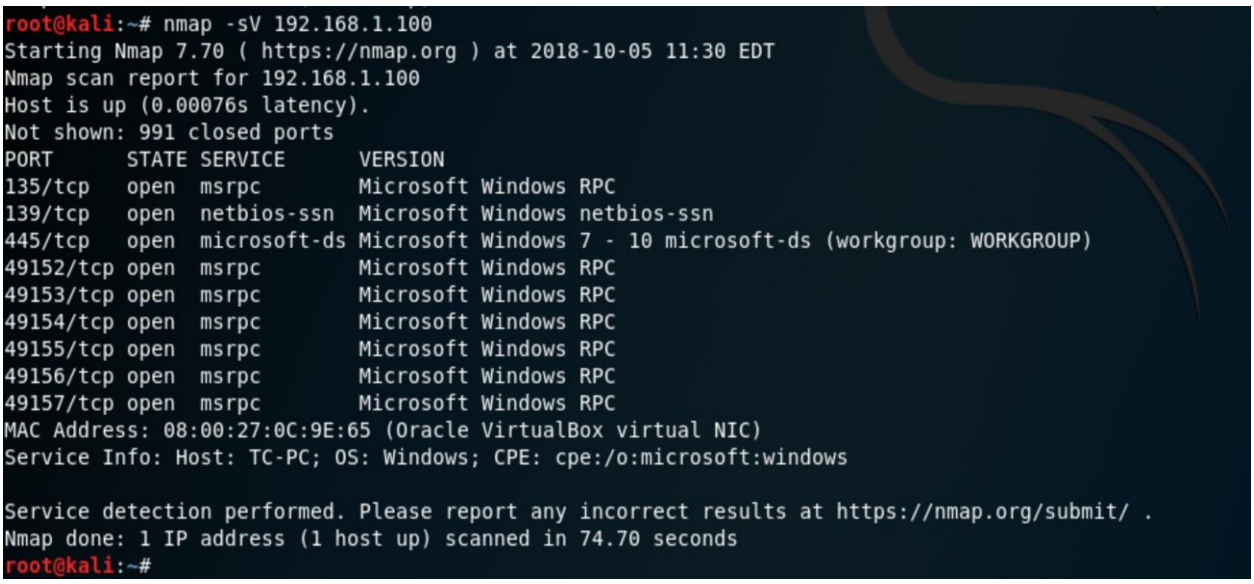
Sev	Name	Family	Count
MEDIUM	SMB Signing not required	Misc.	1
INFO	DCE Services Enumeration	Windows	8
INFO	Nessus SYN scanner	Port scanners	3
INFO	Microsoft Windows SMB Service Detection	Windows	2
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	Link-Local Multicast Name Resolution (LLMNR) Detect...	Service detection	1
INFO	Microsoft Windows SMB Log In Possible	Windows	1

Screen Shots: NMAP

3-1: Nmap -O (Scan that show Operating System Information)



3-2: Nmap -sV (Scan to show open TCP ports and the services and version)



3-3: NMAP -sO (Scan to show IP protocols in use)

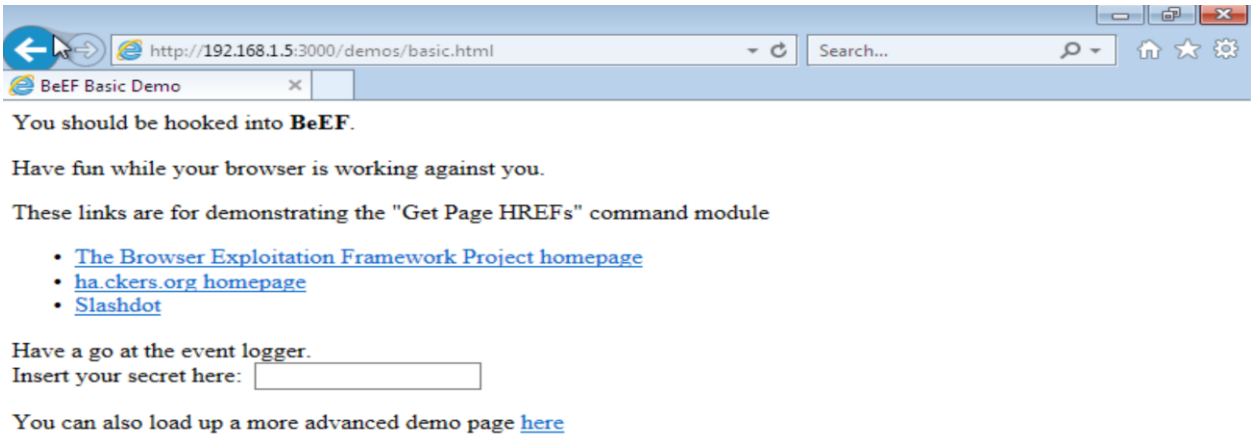
```
root@kali:~# nmap -sO 192.168.1.100
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-05 11:44 EDT
Nmap scan report for 192.168.1.100
Host is up (0.00088s latency).
Not shown: 145 closed protocols, 108 open|filtered protocols
PROTOCOL STATE SERVICE
1        open  icmp
6        open  tcp
17       open  udp
MAC Address: 08:00:27:0C:9E:65 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 20.82 seconds
root@kali:~#
```

3-4: Nmap -sU (scan to show open UDP ports)

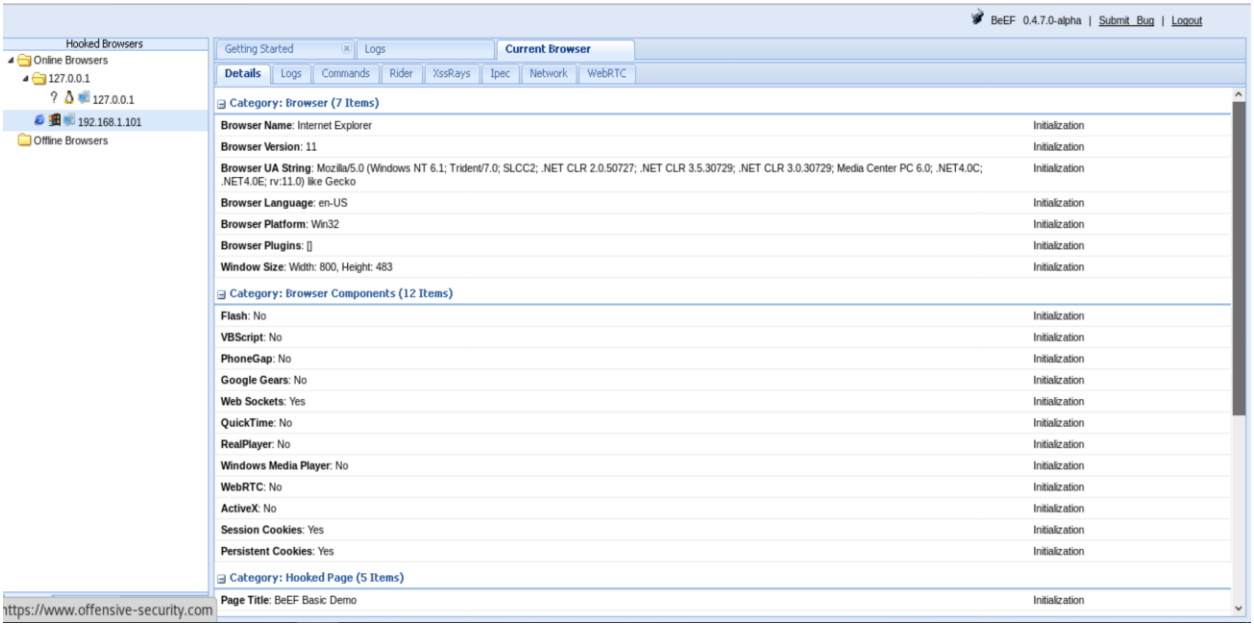
```
root@kali:~# nmap -sU 192.168.1.100
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-05 11:52 EDT
Nmap scan report for 192.168.1.100
Host is up (0.00084s latency).
Not shown: 974 closed ports
PORT      STATE         SERVICE
123/udp   open|filtered ntp
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
207/udp   open|filtered at-7
500/udp   open|filtered isakmp
1060/udp  open|filtered polestar
1645/udp  open|filtered radius
2161/udp  open|filtered apc-2161
4500/udp  open|filtered nat-t-ike
5010/udp  open|filtered telelpathstart
5355/udp  open|filtered llmnr
8001/udp  open|filtered vcom-tunnel
9020/udp  open|filtered tambora
16862/udp open|filtered unknown
16919/udp open|filtered unknown
17205/udp open|filtered unknown
20851/udp open|filtered unknown
21212/udp open|filtered unknown
21354/udp open|filtered unknown
22996/udp open|filtered unknown
28973/udp open|filtered unknown
33717/udp open|filtered unknown
40116/udp open|filtered unknown
49259/udp open|filtered unknown
59846/udp open|filtered unknown
62287/udp open|filtered unknown
MAC Address: 08:00:27:0C:9E:65 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 71.90 seconds
root@kali:~#
```

Screen Shots: BeEF

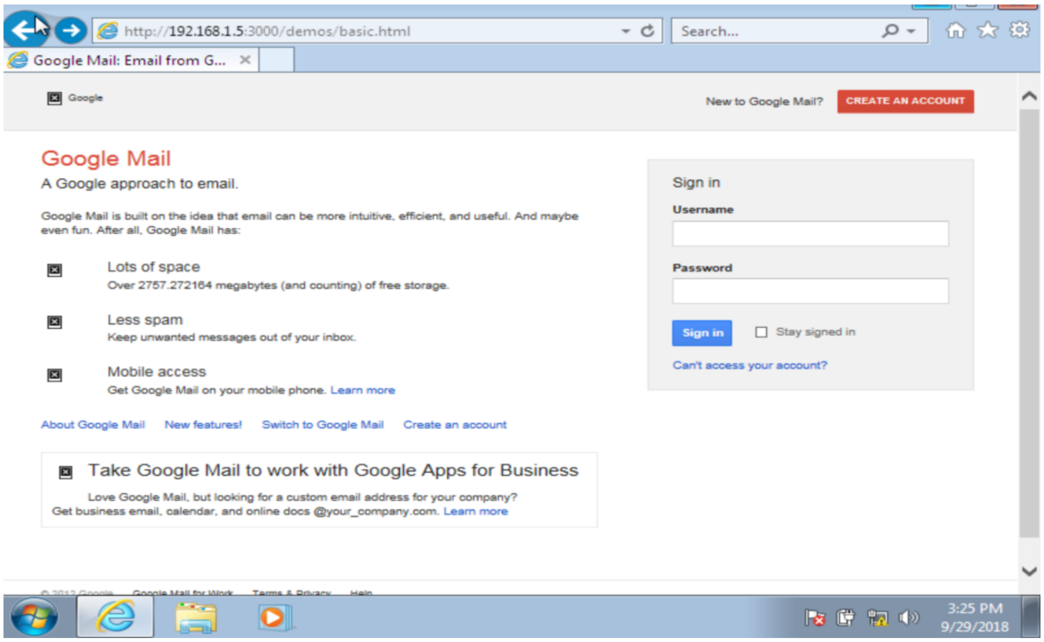
4-1: Demo, getting Hooked



4-2: Information about hooked browser

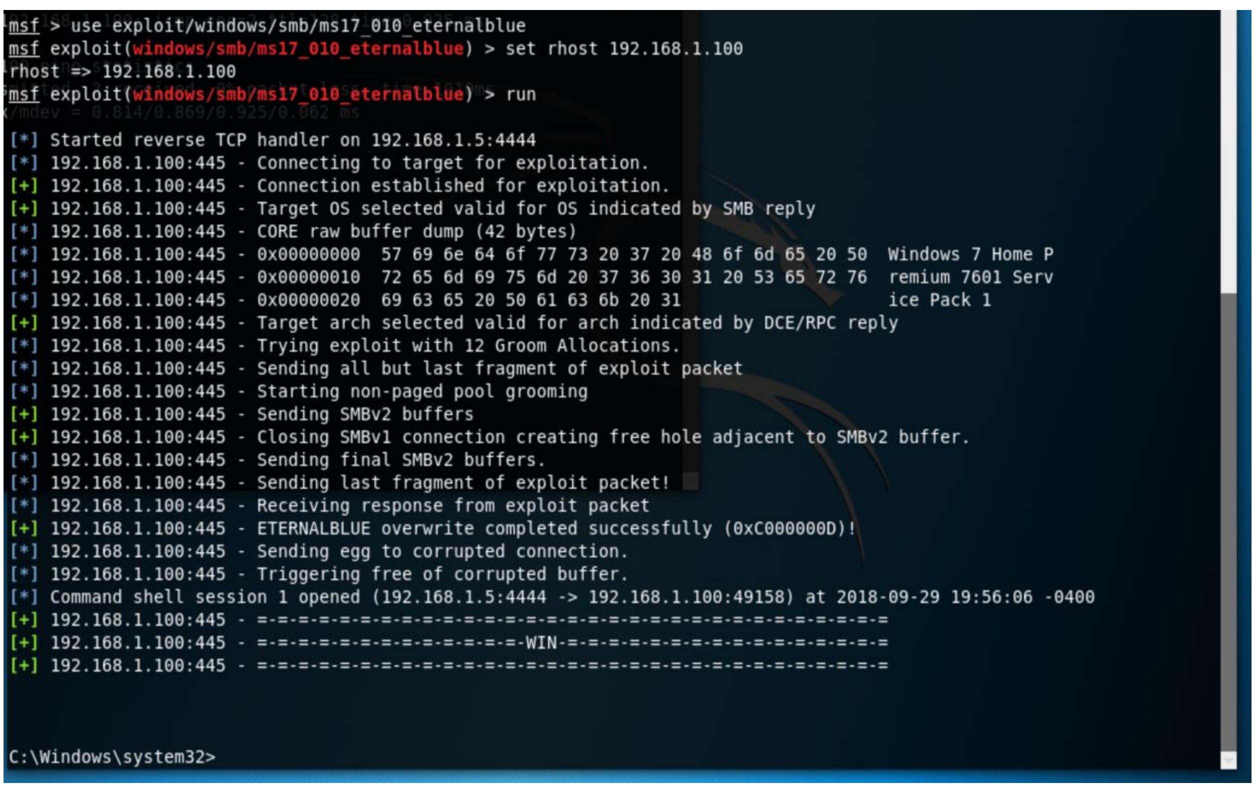


4-3: Example of phishing attacked carried out through hooked browser



Screen Shots: Metasploit

5-1: Configuring Metasploit to use Eternal Blue exploit and executing



Bibliography

Kali. (n.d.). Retrieved Oct 1, 2018, from Kali.org: https://www.kali.org/downloads/

Klosowski, T. (2016, Oct 27). *How to use Nessus to scan a network for vulnerabilities*. Retrieved Oct 1, 2018, from Lifehacker.com: https://lifehacker.com/how-to-use-nessus-to-scan-a-network-for-vulnerabilities-1788261156

Metasploit. (n.d.). Retrieved Oct 1, 2018, from Metasploit.com: https://metasploit.help.rapid7.com/docs

Nmap Network Scanning. (n.d.). Retrieved Oct 1, 2018, from NMAP.org: https://nmap.org/book/man-briefoptions.html

Occupytheweb. (2015, Feb 20). *How to hack web browsers with BeEF*. Retrieved Oct 1, 2018, from null-byte.wonderhowto.com: https://null-byte.wonderhowto.com/how-to/hack-like-pro-hack-web-browsers-with-beef-0159961/

SystemTools. (n.d.). Retrieved Oct 1, 2018, from SystemTools.com: https://systemtools.com/somarsoft/?somarsoft.com

Using the "NSA" EternalBlue exploit on Metasploitable 3. (2017, June 12). Retrieved Oct 1, 2018, from cyberarms.wordpress.com: https://cyberarms.wordpress.com/2017/06/12/using-the-nsa-eternalblue-exploit-on-metasploitable-3/