7.4 Pass-the-Hash

When you login to a Windows host, your password is hashed and compared to a stored hash of your password. If they match, you're in. When you attempt to access a resource on the same Windows domain, the stored hash is sent to the other host and used to authenticate you. With access to these hashes, you can use this mechanism to take over other hosts on the same domain. This is called a pass-the-hash attack.

Use Login -> psexec to attempt a pass-the-hash attack against another Windows host. Click Check all Credentials to have Armitage try all hashes and credentials against the host.

The pass-the-hash attack attempts to upload a file and create a service that immediately runs. Only administrator users can do this. Further, your targets must be on the same active directory domain for this attack to work.

7.5 Using Credentials

Armitage will create a Login menu on each host with known services. Right-click a host and navigate to Login -> service. This will open a dialog where you may choose a username and password from the credentials known to Metasploit.

Some services (e.g., telnet and ssh) will give you a session when a login succeeds. Others will not.

Check the Try all credentials option and Metasploit will login to the service with each of the known credentials. Metasploit automatically adds each successful login to the credentials table for you.

The best way into a network is through valid credentials. Remember that a successful username/password combination from one service may give you access to another host that you couldn't exploit.

7.6 Password Brute Force

Metasploit can attempt to guess a username and password for a service for you. This capability is easy to use through the module browser.

Metasploit supports brute forcing through the auxiliary modules named service\_login. Type login in the module browser to search for them.

To brute force a username and password over SSH, browse to auxiliary/scanner/ssh/ssh\_login in the modules panel and double click it.

If you know the username, set the USERNAME variable. If you'd like Metasploit to brute force the username, select a value for USER\_FILE. Double click the USER\_FILE variable to bring up a file chooser where you can select a text file containing a list of usernames.

Metasploit has many files related to brute forcing in the [metasploit install]/data/wordlists directory.

Set the PASS\_FILE variable to a text file containing a list of passwords to try.

If you're only brute forcing one host and you have a lot of usernames/passwords to try, I recommend using an external tool like Hydra. Metasploit does not make several parallel connections to a single host to speed up the process. This lesson can be taken one step further--use the right tool for each job.

8. Team Metasploit

8.1 Remote Connections

You can use Armitage to connect to an existing Metasploit instance on another host. Working with a remote Metasploit instance is similar to working with a local instance. Some Armitage features require read and write access to local files to work. Armitage's team server adds these features and makes it possible for Armitage clients to use Metaspoit remotely.

Connecting to a remote Metasploit requires starting a Metasploit RPC server and Armitage's team server server.

8.2 Multi-Player Metasploit Setup

The Armitage Linux package comes with a teamserver script that you may use to start Metasploit's RPC daemon and Armitage's team server with one command. To run it:

cd /path/to/armitage

./teamserver [external IP address] [password]

Note: On Kali Linux, Armitage is installed in /usr/share/armitage

This script assumes armitage.jar is in the current folder. Make sure the external IP address is correct (Armitage doesn't check it) and that your team can reach port 55553 on your attack host. That's it.

Metasploit's RPC daemon and the Armitage team server are not GUI programs. You may run these over SSH.

The Armitage team server communicates over SSL. When you start the team server, it will present a server fingerprint. This is a SHA-1 hash of the server's SSL certificate. When your team members connect, Armitage will present the hash of the certificate the server presented to them. They should verify that these hashes match.

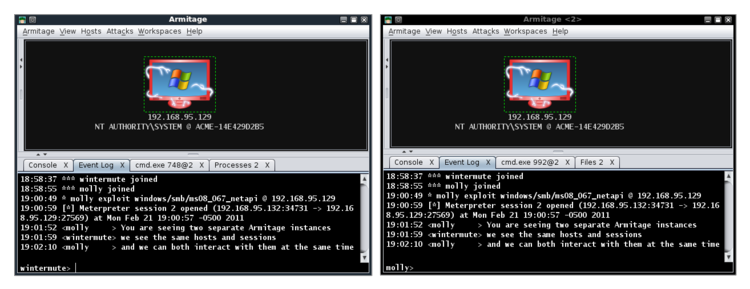
Do not connect to 127.0.0.1 when a teamserver is running. Armitage uses the IP address you're connecting to determine whether it should use SSL (teamserver, remote address) or non-SSL (msfrpcd, localhost). You may connect Armitage to your teamserver locally, use the [external IP address] in the Host field.

Armitage's red team collaboration setup is CPU sensitive and it likes RAM. Make sure you have 1.5GB of RAM in your team server.

8.3 Multi-Player Metasploit

Armitage's red team collaboration mode adds a few new features. These are described here:

View -> Event Log opens a shared event log. You may type into this log and communicate as if you're using an IRC chat room. In a penetration test this event log will help you reconstruct major events.



Multiple users may use any Meterpreter session at the same time. Each user may open one or more command shells, browse files, and take screenshots of the compromised host.

Metasploit shell sessions are automatically locked and unlocked when in use. If another user is interacting with a shell, Armitage will warn you that it's in use.

Some Metasploit modules require you to specify one or more files. If a file option has a ? next to it, then you may double-click that option name to choose a local file to use. Armitage will upload the chosen local file and set the option to its remote location for you. Generally, Armitage will do its best to move files between you and the shared Metasploit server to create the illusion that you're using Metasploit locally.

Penetration testers will find this feature invaluable. Imagine you're working on a pen test and come across a system you don't know much about. You can reach back to your company and ask your local expert to load Armitage and connect to the same Metasploit instance. They will immediately have access to your scan data and they can interact with your existing sessions... seamlessly.

Or, imagine that you're simulating a phishing attack and you get access to a host. Your whole team can now work on the same host. One person can search for data, another can set up a pivot and search for internal hosts to attack, and another can work on persistence. The sky is the limit here.

Some meterpreter commands may have shortened output. Multi-player Armitage takes the initial output from a command and delivers it to the client that sent the command. Additional output is ignored (although the command still executes normally). This limitation primarily affects long running meterpreter scripts.

9. Scripting Armitage

9.1 Cortana

Armitage includes Cortana, a scripting technology developed through DARPA's Cyber Fast Track program. With Cortana, you may write red team bots and extend Armitage with new features. You may also make use of scripts written by others.

Cortana is based on Sleep, an extensible Perl-like language. Cortana scripts have a .cna suffix.

Read the Cortana Tutorial to learn more about how to develop bots and extend Armitage.

9.2 Stand-alone Bots

A stand-alone version of Cortana is distributed with Armitage. You may connect the stand-alone Cortana interpreter to an Armitage team server.

Here's a helloworld.cna Cortana script:

on ready {

println("Hello World!");

quit();

}

To run this script, you will need to start Cortana. First, stand-alone Cortana must connect to a team server. The team server is required because Cortana bots are another red team member. If you want to connect multiple users to Metasploit, you have to start a team server.

Next, you will need to create a connect.prop file to tell Cortana how to connect to the team server you started. Here's an example connect.prop file:

host=127.0.0.1

port=55553

user=msf

pass=password

nick=MyBot

Now, to launch your bot:

cd /path/to/metasploit/msf3/data/armitage

java -jar cortana.jar connect.prop helloworld.cna

9.3 Script Management

You don't have to run Cortana bots stand-alone. You may load any bot into Armitage directly. When you load a bot into Armitage, you do not need to start a teamserver. Armitage is able to deconflict its actions from any loaded bots on its own.

You may also use Cortana scripts to extend Armitage and add new features to it. Cortana scripts may define keyboard shortcuts, insert menus into Armitage, and create simple user interfaces.

To load a script into Armitage, go to Armitage -> Scripts. Press Load and choose the script you would like to load. Scripts loaded in this way will be available each time Armitage starts.

Output generated by bots and Cortana commands are available in the Cortana console. Go to View -> Script Console.

9.4 Resources

Cortana is a full featured environment for developing red team bots and extending Armitage. If you'd like to learn more, take a look at the following resources:

Cortana Tutorial for Scripters

Public Cortana Script Repository

Sleep Manual

7.4 通过散列

当你登录到 Windows 主机时，您的密码散列，并与存储的哈希密码的相比。如果它们匹配，你的。当您尝试访问相同的 Windows 域上的资源时，存储的哈希是发送到其他主机，用于验证您的身份。与访问这些哈希值，你可以使用这种机制接管其他主机位于相同的域。这就被所谓通过散列攻击。

使用登录-> psexec 尝试另一个 Windows 主机通过散列攻击。单击检查所有凭据有阿米蒂奇尝试所有哈希和针对主机凭据。

通过散列攻击试图上载文件和创建立即运行的服务。只有管理员用户才可以这样做。进一步，你的目标必须是在同一 active directory 域为此攻击上班。

7.5 使用凭据

阿米塔吉将与已知服务每个主机上创建一个登录菜单。右键单击主机，然后导航到登录-> 服务。这将打开一个对话框，您可能选择一个用户名和密码从已知的 Metasploit 的凭据。

某些服务 (如 telnet 和 ssh) 会给你一个会话，当登录成功。别人不会。

检查所有凭据选项和 Metasploit 将是使用每个已知的凭据都登录到服务的尝试。Metasploit 自动表中添加每个成功的登录凭据为你。

进入网络的最佳方法是通过有效的凭据。记得从一个服务成功用户名/密码组合可能让您可以访问另一台主机，你不能利用。

7.6 密码暴力破解

Metasploit 可以尝试猜一个用户名和密码为你提供服务。这种能力是通过模块浏览器的易用。

Metasploit 支持蛮力破解通过名为 service\_login 的辅助模块。键入登录模块浏览器搜索它们。

蛮力的用户名和密码通过 SSH，浏览到辅助/扫描仪/ssh/ssh\_login 模块面板中，双击它。

如果你知道用户名，设置用户名变量。如果你想去 Metasploit 蛮力的用户名，选择一个值为 USER\_FILE。双击 USER\_FILE 变量，弹出一个文件选择器，您可以在其中选择一个包含用户名的列表的文本文件。

Metasploit 有许多相关的蛮力破解 [metasploit 安装] / 数据/单词表目录中的文件。

将 PASS\_FILE 变量设置为一个文本文件，包含列表的密码尝试。

如果你只是蛮迫使一个主机和你有很多的用户名/密码尝试，建议您使用外部工具似长蛇。Metasploit 不会几个并行连接到单个主机，加快这一进程。这节课可以采取一步进一步 — — 为每个作业使用合适的工具。

8.团队 Metasploit

8.1 远程连接

阿米塔吉可用于连接到另一台主机上的现有 Metasploit 实例。使用远程 Metasploit 实例是类似于使用本地实例。有些阿米蒂奇功能需要读取和写入访问到本地的文件工作。阿米塔吉团队服务器添加这些特性，使得阿米蒂奇客户端使用 Metaspoit 远程。

连接到远程的 Metasploit 需要开始 Metasploit RPC 服务器和阿米塔吉团队服务器服务器。

8.2 多玩家 Metasploit 安装程序

阿米蒂奇 Linux 包装带有一个 teamserver 脚本，您可以使用启动 Metasploit 的 RPC 守护进程和阿米塔吉团队服务器使用一个命令。要运行它︰

cd /path/to/armitage

./ teamserver [外部 IP 地址] [密码]

注︰ 卡莉在 Linux 上，阿米塔吉被安装在 /usr/share/armitage

此脚本假定 armitage.jar 是当前文件夹中。请确保外部的 IP 地址是否正确 （阿米塔吉不检查它） 和您的团队可以达到你攻击主机上的端口 55553。就是这样。

Metasploit 的 RPC 守护进程和阿米蒂奇团队服务器不是 GUI 程序。您可以运行这些通过 SSH。

阿米蒂奇团队服务器通过 SSL 通信。当你开始团队服务器时，它将当前服务器指纹。这是服务器的 SSL 证书的 sha-1 哈希。当您的团队成员连接时，阿米塔吉将向他们提出向服务器出示证书的哈希。他们应验证这些哈希值匹配。

运行 teamserver 时，不连接到 127.0.0.1。阿米蒂奇使用您要连接的 IP 地址来确定是否它应使用 SSL （teamserver，远程地址） 或非 SSL （msfrpcd，本地主机）。您可能连接阿米蒂奇到你本地的 teamserver，在主机字段中使用 [外部 IP 地址]。

阿米塔吉红队协作安装程序是 CPU 敏感和它喜欢 RAM。请确保在您的团队服务器有 1.5 GB 的 RAM。

8.3 多玩家 Metasploit

阿米塔吉红队协作模式添加了几个新功能。在这里介绍这些︰

查看-> 事件日志打开共享的事件日志。你可能在此日志中键入和交流，如果你使用 IRC 聊天室。在渗透测试此事件日志将帮助你重建重大事件。

多个用户可以同时使用 Meterpreter 的任何会话。每个用户可以打开一个或多个命令外壳、 浏览文件，和截图受损主机。

Metasploit shell 会话是自动锁定和未锁定在使用时。如果另一个用户正在与壳进行交互，阿米蒂奇将警告您，它是在使用中。

一些 Metasploit 模块要求您指定一个或多个文件。如果一个文件选项了吗？在它旁边，然后您可以双击该选项名称，选择要使用的本地文件。阿米蒂奇将选定的本地文件上传和到远程位置为您设置的选项。一般，阿米蒂奇将尽其所能你和共享的 Metasploit 服务器使人产生幻觉，你使用 Metasploit 本地之间移动文件。

渗透测试人员会发现这项功能非常宝贵。想象一下你正在笔测试和遇到你不知道很多关于系统。你可以到达回到您的公司，问你当地的专家来加载阿米蒂奇和连接到相同的 Metasploit 实例。他们将立即访问您的扫描数据和他们可以与您现有的会话...交互无缝。

或者，想象一下，你就在模拟网络钓鱼攻击，您可以访问到主机。你的整个团队现在可以在同一台主机工作。一个人可以搜索数据，另一个可以设置数据透视和搜索的内部主机的攻击，和另一个可以坚持工作。天空才是极限在这里。

一些 meterpreter 命令可能缩短输出。多玩家阿米蒂奇需要命令的初始输出和将其传递给客户端发送的命令。（虽然通常仍执行命令），额外的输出将被忽略。这种限制主要影响长时间运行 meterpreter 脚本。

9.脚本阿米蒂奇

9.1 柯塔娜

阿米蒂奇包括柯塔娜，通过 DARPA 的网络快速跟踪计划开发一种脚本技术。与柯塔娜，你可能会写红队机器人和延长阿米蒂奇与新功能。您也可以使用脚本由别人写。

柯塔娜基于可扩展的 Perl 类似语言的睡眠。柯塔娜脚本有一个.cna 后缀。

阅读柯塔娜教程来了解更多关于如何开发机器人和扩展阿米蒂奇。

9.2 独立的机器人

柯塔娜单机版分布与阿米蒂奇。你可以连接独立的柯塔娜翻译到阿米蒂奇团队服务器。

这里是 helloworld.cna 柯塔娜脚本︰

在准备好 {

println ("Hello World ！");

quit （);

}

若要运行此脚本，您将需要启动柯塔娜。第一，独立的柯塔娜必须连接到团队开发服务器。团队服务器是必需的因为柯塔娜机器人是另一个红色的团队成员。如果你想要将多个用户连接到 Metasploit，你不得不开始团队开发服务器。

接下来，您将需要创建一个 connect.prop 文件来告诉柯塔娜如何连接到团队服务器你开始。这里是 connect.prop 文件的示例︰

主机 = 127.0.0.1

端口 = 55553

用户 = 无国界医生组织

通过 = 密码

尼克 = MyBot

现在，启动你的机器人︰

cd /path/to/metasploit/msf3/data/armitage

java-jar cortana.jar connect.prop helloworld.cna

9.3 脚本管理

你不需要运行独立的柯塔娜机器人。你可能会直接加载到阿米蒂奇的任何 bot。Bot 加载到阿米蒂奇时，你不需要启动 teamserver。阿米蒂奇是能够消除它从任何加载的机器人在其自己的行动。

您还可以使用柯塔娜脚本扩展阿米蒂奇，向其添加新功能。柯塔娜脚本可能定义键盘快捷键、 菜单插入阿米蒂奇，和创建简单的用户界面。

将脚本加载到阿米蒂奇，阿米蒂奇去-> 脚本。按负荷并选择您想要加载的脚本。以这种方式加载的脚本将每次阿米蒂奇启动的时可用。

由机器人和柯塔娜命令生成的输出是柯塔娜控制台中可用。转到视图-> 脚本控制台。

9.4 资源

柯塔娜是完整的特色的环境发展红队机器人和延长阿米蒂奇。如果你想要了解更多，看看以下资源︰

脚本编写者柯塔娜教程

公共柯塔娜脚本存储库

睡眠手册

[https://ssl.translatoruser.net/static/242031/img/tooltip_logo.gif](http://www.bing.com/translator)https://ssl.translatoruser.net/static/242031/img/tooltip_close.gif

**原文**

First, stand-alone Cortana must connect to a team server.