www.og150.com

Automated Penetration Test

TABLE OF CONTENTS

www.og150.com

Introduction.

The OG150 is pre-configured with scripts that enable the user to launch an automated penetration test against the network infrastructure where it has been deployed. A penetration test, in simple terms, can be described as a method of evaluating the security of a computer system or network. The tests performed by the OG150 are **NOT** all-encompassing and should not be viewed as a direct replacement for a full scale penetration test performed by a certified/experienced Security Consultant. It does, however, provide useful information about the target infrastructure which may allow more focussed attacks to be launched.

Test Structure.

The OG150 is pre-configured to execute 11 tests by default. It is important to stress that these tests are modular and can be added to very easily. If you do create your own test, please share them with me so that the wider community can benefit! The result of each test is displayed in a consolidated 'Security Report'. The 11 default tests are summarised below:

- **DISPLAY OG150 IP DETAILS** – Displays the IP address assigned to the OG150 via DHCP. This is useful to map out the IP structure of the target infrastructure.
- **VERIFY ICMP CONNECTIVITY TO THE INTERNET** – Attempts to ping www.google.com. This is useful to determine if ICMP traffic is permitted by the firewall.
- **TRACEROUTE TO THE INTERNET** – Attempts to traceroute to www.google.com. This is useful to map out the IP structure of the target infrastructure.
- **DISCOVER HOSTS AND SERVICES ON THE LOCAL NETWORK USING NMAP** – Performs an NMAP scan against the OG150s local subnet. This is useful to determine what services are running on host machines.
- **CDP (Cisco Discovery Protocol) SNOOPING** – Listens for CDP messages. This protocol can leak sensitive information about Cisco network infrastructure devices – for example, switches.
- **FHRP (First Hop Redundancy Protocol) SNOOPING** – Listen for FHRP messages. If detected, FHRP attacks can be launched resulting in MITM (Man In The Middle) or DOS (Denial of Service) attacks.
- **DYNAMIC ROUTING PROTOCOL SNOOPING** – Listen for dynamic routing protocol messages. If detected, routing protocol attacks can be launched resulting in MITM (Man In The Middle) or DOS (Denial of Service) attacks.
- **NBTSCAN (NETBIOS SCAN)** – Lists important information about users and/or devices. This can be used for further, more focussed, attacks.
- **WIRELESS NETWORK SCANNING** – Lists any wireless networks within range of the OG150. This can be used for a range of attacks against the wireless infrastructure.
- **PUBLIC IP ADDRESS INFORMATION** – Provides details about the public IP address used by the target infrastructure. This can be later used for external attacks.
- **REMOTE ACCESS STATUS** – Confirms whether a reverse SSH connection has been successfully established.

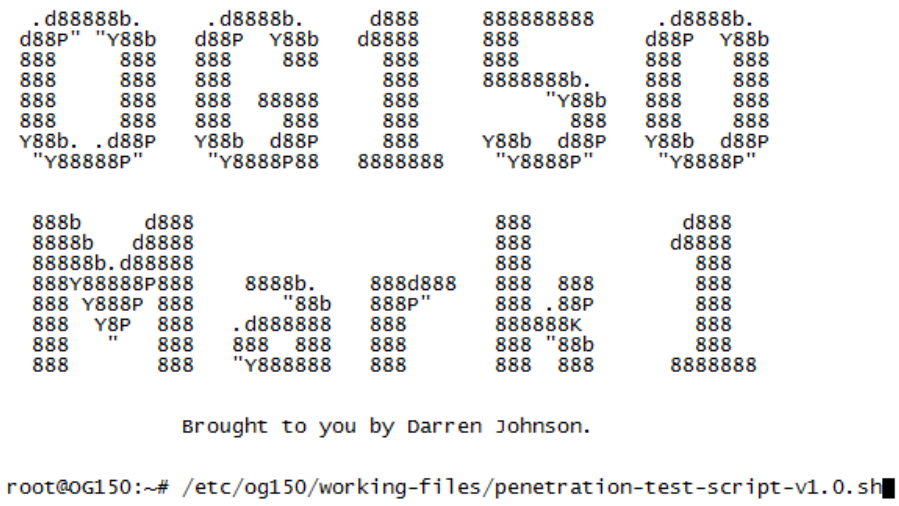
www.og150.com

Follow @theog150

Manually Launching The Automated Penetration Test.

The easiest way to launch the automated penetration test is **MANUALLY**. Once the OG150 has been connected to the target network infrastructure, you simply need to connect to it (using SSH) and launch the automated penetration test script. Screenshot 1 shown below demonstrates the command that will execute the automated penetration test script.

Screenshot 1 – Execute the automated penetration test script



The time it takes for the penetration test to complete depends on the size of the target infrastructure. During my own testing, this time varies between 5-10 minutes.

You can monitor progress of the penetration test. To do this, establish a second SSH connection to the OG150, and enter 'logread –f' as shown Screenshot 2. The log will update in real-time and confirms when each individual test has completed. To exit 'logread' enter 'CTRL+C'.

Screenshot 2 – Monitoring progress of the automated penetration test

```
root@OG150:~# logread -f
Mar 16 13:14:03 OG150 user.notice root: OG150 Penetration Test has started
Mar 16 13:14:11 OG150 user.notice root: OG150 'DISPLAY OG150 IP DETAILS' test is completed
Mar 16 13:14:17 OG150 user.notice root: OG150 'TRACEROUTE TO THE INTERNET' test is completed
Mar 16 13:14:17 OG150 user.notice root: OG150 'VERIFY ICMP CONNECTIVITY TO THE INTERNET' test is completed
```

Once the automated penetration test is finished, you will see output similar to that shown in Screenshot 3.

Screenshot 3 – Screen output when the automated penetration test has finished

Every 'Security Report' is archived with a date/timestamp in the following location: '/etc/og150/archived-security-reports/'. You can list the 'Security Reports' in the archive as shown is Screenshot 4. Note: It is important to regularly delete old 'Security Reports' otherwise you will eventually run out of memory space.

Screenshot 4 – Display the archived 'Security Reports'

```
root@OG150:~# ls -l /etc/og150/archived-security-reports/
-rw-r--r--    1 root     root         40366 Mar 16 13:19 OG150-Security-Report-13:19:06-Sat-16-Mar-2013
root@OG150:~#
```

To open the 'Security Report', you can use the 'cat' command as shown in Screenshot 5. Personally, I prefer to transfer the 'Security Report' to my laptop using WinSCP and view it from there.

Screenshot 5 – Open a 'Security Report' using the 'cat' command

```
root@OG150:~# cat /etc/og150/archived-security-reports/OG150-Security-Report-13\:19\:06-Sat-16-Mar-2013
```

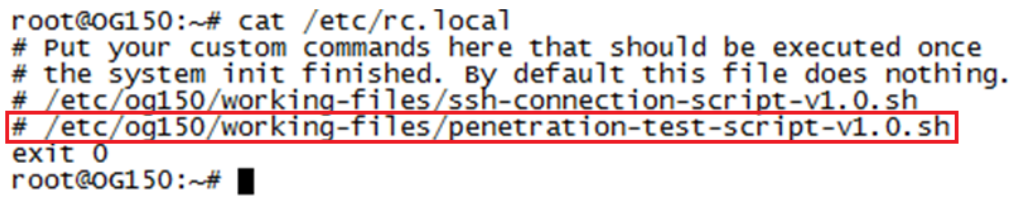
Automatically Launching The Automated Penetration Test On Boot.

A more covert way to launch the automated penetration test is automatically upon bootup. All this requires is that the user plugs the OG150 into the target infrastructure, waits approximately 10 minutes (time duration to complete the automated penetration test varies depending on the size of the target network) and then removes the OG150. The user can then view the 'Security Report' when they get back to the privacy of their office/home.

So, how do you do this? The 'rc.local' file executes near the end of the boot process. You can add scripts to this file which will result in the scripts being executed each time the OG150 boots (due to a power cycle, reboot, etc).

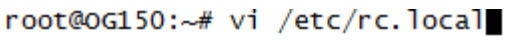
The default contents of the 'rc.local' file is displayed in Screenshot 6. As you can see, the automated penetration script (shown earlier in Screenshot 1) IS included in the 'rc.local' file, however it is prepended with a '#' - which means it is effectively ignored.

Screenshot 6 – Default 'rc.local' file contents



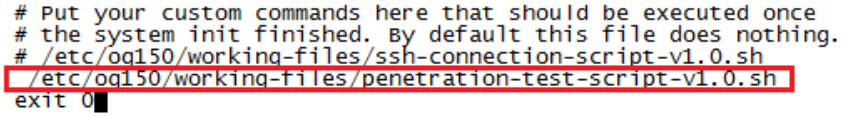
To ensure that the automated penetration script is executed as part of the boot sequence, we simply need to remove the '#' for the automated penetration script. Although there are a few ways to do this, the simplest way is to use the 'vi' program. In simple terms, 'vi' is a text editor and allows you to change the contents of a file from a CLI (SSH) session. This first step is to open the file with 'vi' as shown in Screenshot 7.

Screenshot 7 – Open 'rc.local' file with 'vi'



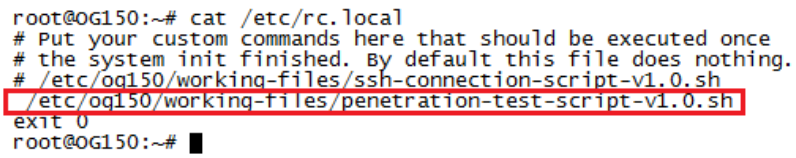
The full tutorial on the use of 'vi' is outside the scope of this guide, there are lots of references online regarding this subject. This guide will illustrate the steps to make and save changes to a file. Once the file is opened with 'vi', pressing 'CTRL+i' will allow you to make changes to the file. Use the cursor keys to move up, down, left and right. You can now navigate to the automated penetration script line and delete the '#' as shown in Screenshot 8.

Screenshot 8 – Editing 'rc.local' file using 'vi'



In order to save the changes, you need to exit out of the editing mode, to do this press 'ESC'. Next type ':wq' and then a carriage return to save the changes. Finally, verify the changes have been applied using the 'cat' command shown in Screenshot 9.

Screenshot 9 – Verify 'rc.local' file changes



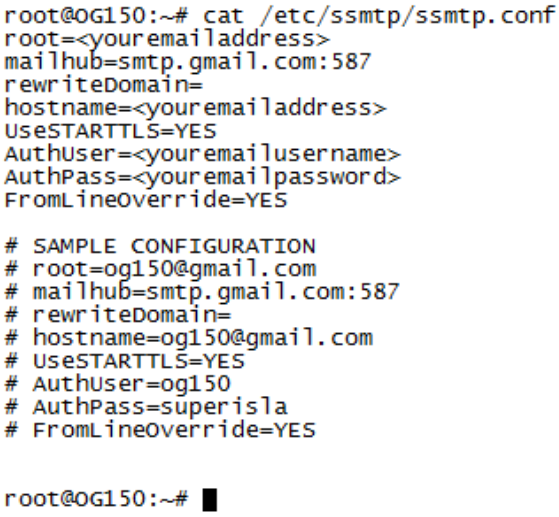
To test this functionality, simply power cycle the OG150. Once booted you can SSH to the OG150 and monitor progress of the automated penetration test, as previously shown in Screenshot 2. You now have a simple, automated, penetration testing drop box that only needs to be connected to a target network for a very short time – very covert and very useful.

BONUS – Email 'Security Report' Directly To You!

Another useful feature is to automatically email the 'Security Report' to you once it is complete. This means you don't have to login to the OG150 to retrieve the content. This is relatively simple to set up and for best results I recommend using Gmail for the OG150 email account. Note: I have tried other email providers – Yahoo for example – with mixed results, bottom line is that Gmail works best.

The first step to configure the SSMTP config file. This is the email (Gmail) account that the OG150 will use to email you the 'Security Report' results. Screenshot 10 illustrates the default SSMTP config file. A sample configuration is provided at the bottom of this config file to assist with the configuration

Screenshot 10 – Default SSMTP configuration



Although there are a few ways to edit this configuration file, the simplest way is to use the 'vi' program. Assuming you are using Gmail, the only variables that should differ from the 'SAMPLE CONFIGURATION' shown in Screenshot 10 are:

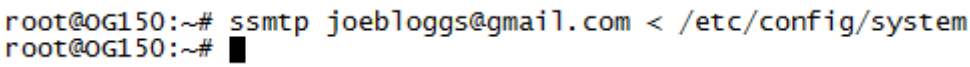
```
root=<enter your full Gmail address here>
hostname=<enter your full Gmail address here>
AuthUser=<enter your Gmail username here>
AuthPass=<enter your Gmail password here>
```

Screenshot 11 shows the edited configuration (with censoring to protect my own credentials).

Screenshot 11 – Edited SSMTP configuration

You can now test this functionality to ensure that the OG150 is able to send emails using the configured Gmail account. An example test is demonstrated in Screenshot 12. As you can see, the OG150 will send the contents of the '/etc/config/system' file to the email address joebloggs@gmail.com. If you receive the test email your SSMTP configuration is working and you can proceed to the final step.

Screenshot 12 – SSMTP test



The final step is to edit the automated penetration test script to include the email destination. Once this is done, the OG150 will email the contents of the 'Security Report' to this email address. The automated penetration test script is a large file, if you display the contents using the command 'cat /etc/og150/working-files/penetration-test-script-v1.0.sh' you will see the SSMTP configuration near the end of the script as shown in Screenshot 13.

Screenshot 13 – SSMTP configuration in the automated penetration test script

You need to change the “your email address” to the actual destination email address (where you want to email the ‘Security Report’ to). Although there are a few ways to do this, the simplest way is to use the ‘vi’ program.

Screenshot 14 – Automated penetration test script will send the ‘Security Report’ to my <censored>@yahoo.co.uk email address

Once these changes have been made, you are done ☺ You now simply need to invoke the automated penetration test script and you will receive the ‘Security Report’ via email. It is important to highlight that it does NOT matter if you invoke the automated penetration test script manually or automatically – you will ALWAYS be emailed the ‘Security Report’ if it has been configured. Screenshot 15 illustrates a ‘Security Report’ that was emailed to me and viewed on my iPhone.

Screenshot 15 – ‘Security Report’ email received on iPhone