FANSHAWE

INFO-6065

Ethical Hacking & Exploits

Mobile Devices

Agenda

- Test 02 – Next week!
- Mobile Devices
- Device Risks
- Application Risks
- Mobile Device Security
- Lab 08 Overview
  - Linux Exploits

Mobile Devices

Devices & Risks

- When we are talking about mobile devices, we are generally thinking about Cell Phones and Tablets
- The risks affecting mobile devices fall into two main categories
  - Device Risks
  - Application Risks

Device & Application Risks

Device Risks

- Risks that are inherent to the devices themselves
- Mobile devices are now basically computers with a different form factor and thus are exposed to similar risks found on computers

Application Risks

- Risks which originating from third party applications
- There is often little the end user can do to really tell what a third party application is doing on their device
  - Permissions during install

Device Risks

Device Risks

Data Storage

Employees may compromise data security by storing sensitive information on their mobile devices

- Allows users to remove data from the organization intentionally or unknowingly
- Allow users to take pictures of sensitive areas
- Could pose compliance risks

Device Risks

Weak Passwords

- Users traditionally use weak passwords with mobile devices
- If they have sensitive data on their device, it is at risk
- Although you can centrally set password policies on some devices it isn't available to all mobile devices
  - Often requires specific infrastructure components
    - BES, Exchange, etc.

Device Risks

WiFi Hijacking

- Taking advantage of free wireless to steal personal information
- Attacks are performed on open hotspots

Open Hotspots

- If a user is connected to the corporate network and allowing people to connect to their mobile device
- Similar to unauthorized APs

Device Risks

Baseband Hacking

- Leveraging the network connection, underlying hardware and firmware that connects to cell towers to attack the voice capabilities of the device
- Calls can be intercepted or eavesdropped upon

Baseband processor SiTel SC14434

https://en.wikipedia.org/wiki/Baseband_processor

Device Risks

NSO Group

- Israeli based company that licenses surveillance software to spy on mobile phones
- Clients include government agencies
- Creators of **Pegasus**

Baseband processor SiTel SC14434

https://en.wikipedia.org/wiki/Baseband_processor

Device Risks

Bluetooth Snooping

- Results from users not resetting their default PINs
- Allows an attacker to pair with the device
- Can be used to eavesdrop on calls or steal data

Bluejacking

- Unsolicited messages are sent to near-by Bluetooth devices
- Specialized antennas can be used to get around proximity requirements for Bluetooth communications

Device Risks

Bluetooth Fuzzing

- Attacks the Bluetooth pairing process
- Invalid data is sent to cause abnormal behavior in the device
  - Crashing
  - Privilege Escalation
  - Intrusions
  - Installation of Malware

Application Risks

Application Risks

Trojaned Apps

- The same as with computers
- A malicious program is installed along with a seeming useful program
- DroidDream is an example of an Android Trojan that was distributed through Google Play
  - Allowed for the stealing of information through opening a backdoor to the device
  - Operated between 11pm and 8am – hence the name

Application Risks

Trojaned Apps

- The same as with computers
- A malicious program is installed along with a seeming useful program
- DroidDream is an example of an Android Trojan that was distributed through Google Play
  - Allowed for the stealing of information through opening a backdoor to the device
  - Operated between 11pm and 8am – hence the name

Application Risks

- Hidden Malicious URLs
  - Shortened links are often used with mobile devices to reduce the amount of text that needs to be entered
    - These shortened URLs could point anywhere
    - bit.ly, tinyURL, etc.
  - It is much more difficult to validate URLs on a mobile device than on a PC
    - Hover over, often results in clicking on the link

Application Risks

- Phishing
  - Same as phishing on PCs
  - Tricking a user into opening an attachment or clicking on a link
- SMiShing
  - Similar to phishing, but uses SMS test messages
- War Texting
  - Takes advantage of smart phone integration into modern vehicles (uses cell signals)
  - Can be used to start, stop, unlock, or track vehicles (OnStar, Assist, etc.)

Mobile Device Security

Device Security

- Mobile device security features fall into three main categories
  - Standalone features built into the device
  - Third party applications added to the device
  - Externally managed features supported by the device
    - Mobile Device Management

Device Security

- Standalone Features
  - Mobile device passwords, patterns, facial recognition etc.
  - Limiting third party applications to those supported by the manufacturer
  - Device encryption
- Third Party Applications
  - Antivirus, Antispam applications
  - Some will block Callers and SMS contacts

Device Security

github.com/mvt-project/mvt

mvt-project / mvt Public

Notifications | Fork 749 | Star 8.4k

Code | Issues 12 | Pull requests 2 | Discussions | Actions | Projects | Security

main | Go to file | Code

DonnchaC Change checksum log message to in... ... 4 days ago 763

.github/workflows	Fixes a bug with YAML parsing of githu...	last week
dev	Removed AUTHORS file in favor of exp...	10 months ago
docs	Update documentation on making bac...	2 weeks ago
mvt	Change checksum log message to info...	4 days ago

About

MVT (Mobile Verification Toolkit) helps with conducting forensics of mobile devices in order to find signs of a potential compromise.

mvt.re

android | security | ios | mobile | forensics | forensics-tools

Device Security

- Mobile Device Management Tools
  - Rely on features built into the device, but are managed externally
  - These would usually be integrated before a device is allowed to connect to the network
  - Can add a wide variety of features
    - Device provisioning and configuration
    - Software distribution
    - Encryption and password management
    - Remote wipe and lock
    - Policy enforcement

MDM Capabilities

Policy Management

- Consistent application of security settings across mobile devices

Security Management

- Enforcement of settings related to authentication and encryption

Software Management

- Controlling the deployment, updating, deletion and blocking of applications

MDM Capabilities

Inventory Management

- Tracking devices, owners and applications
- Can also be used for remote support

Remote Provisioning and De-Provisioning

- Automatic setup of devices when they are joined, and automated wipe of devices when they are removed

Messaging Control

- Applying limitations to email, calendar, SMS, etc.

Data Loss Prevention (DLP)

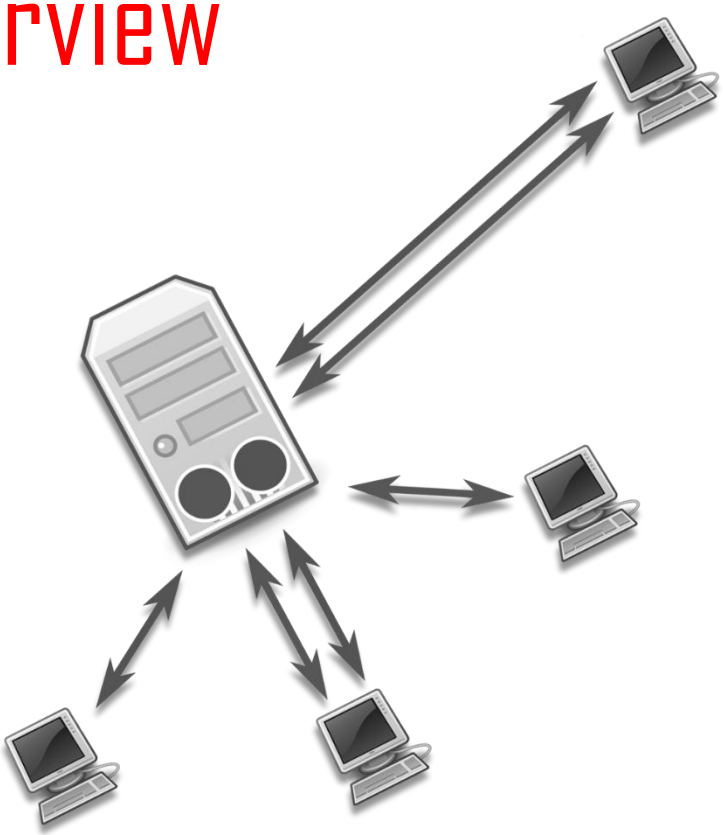
- Control over data that is sent or received from the device to keep it within the organization

MDM Capabilities

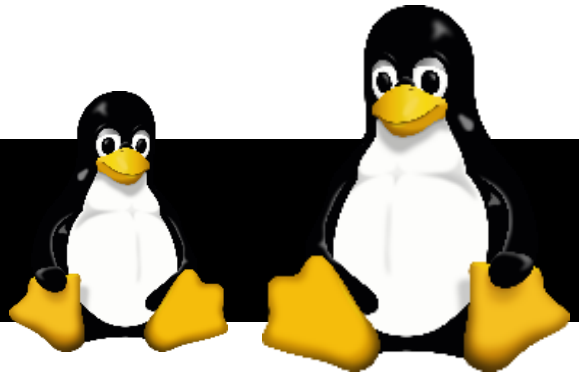
Over-the-air-programming (OTA)

- One of the main components of MDM
- Sends commands a binary Short Messaging Service messages

Lab 08 Overview



Lab 08: Linux Exploits



Part 01: Exploit Distributed Compile System on MS2

Part 02: Exploit Tomcat on MS2

Part 03: Create a webshell

Part 04: Exploit ProFTPD on MS2

Part 05: Escalate to Root Privileges on MS2

WebShells

"Popping a shell" is one of the main objectives of an attacker or pen tester

In addition to the methods we've already observed, another category of shell is one that can be activated over the web

This is typically done by uploading a file to the server and having it activate a shell remotely through the URL

WebShells

Kali Linux comes with several categories of webshells based on the technology used

(aspx, perl, php, etc.)

The **laudanum** repository is used for SQL injection attacks

```
┌──(root㉿artmack)-[/usr/share/webshells]
└─# ls -ail
total 40
1449619 drwxr-xr-x   8 root root  4096 Aug  8  2022 .
 536584 drwxr-xr-x 328 root root 12288 Feb  7 20:41 ..
1449629 drwxr-xr-x   2 root root  4096 Aug  8  2022 asp
1449632 drwxr-xr-x   2 root root  4096 Aug  8  2022 aspx
1449624 drwxr-xr-x   2 root root  4096 Aug  8  2022 cfm
1449621 drwxr-xr-x   2 root root  4096 Aug  8  2022 jsp
1449620 lrwxrwxrwx   1 root root    19 Aug  8  2022 laudanum → /usr/share/laudanum
1449626 drwxr-xr-x   2 root root  4096 Aug  8  2022 perl
1449634 drwxr-xr-x   3 root root  4096 Feb 22 14:18 php
```

WebShells

Depending on the web server, the path to directly accessible resources may be different

Linux:	/var/www/
Windows	inet/pub/wwwroot
Coldfusion	CFIDE

Post Exploit

Privilege Escalation

- Increasing access to that of a user or process with more privileges on the target system

Why Privilege Escalation Techniques are Needed

- Attackers are often targeting less savvy users with limited privileges (e.g. users who will click on links)
- Even if an attacker gets an Admin process on a machine it may not have default access to all the resources the attacker wants