Hacking Hackers

Ashish Mistry

About Me

Ashish Mistry

- Information Security Researcher
- Founder & Director of Jetr Infotech Pvt Ltd
- Team lead of Hcon Security Labs
- Research areas - OSINT, Web, Malware

Warning!

NO 0day inside

Disclaimer

- I am not responsible for whatever you do with this information.
- Views presented here are of my own and doesn't represent my company

About this talk

- Can be taken as idea for making a script
- Just about having fun
- Needs active participation from you

more discussion

=

more awesome talk

Why to hack hackers ?

My reasons

- Hacking bad guys
  - Recovering what is right ethically
- Trolling script monkeys
  - We all need some good times ;)
- Country level #Ops
  - People who makes electronic goods for world

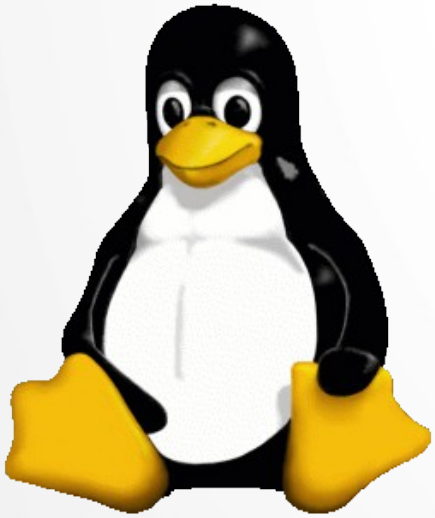
Ways to hack

Method #1

- Infecting a cracked rare / famous security app
  - virus/backdoor use your imagination ;)
- There are many havij, IBM app scan, accunetix, or just making a torrent copy of a tool or a tool pack.

Method #2

- Making and infecting a distro, but infecting some of the core but rarely updated binaries like bash utility commands "ls, cd etc"
  - using veil or backdoor factory
- no one uses antivirus on kali !



Method #3

- Making or faking an exploit available with encoding

  you can't see whats in -> execution -> fun

  - can be done in webapp and linux local root exploits
  - same applies to android local roots
- even the local root is authentic but will be flagged by antivirus so people avoid the detection and run it anyway !

Method #4

- Getting the so called PRIV8 shells

  magic code → encode → distribute → fun

  - online multi encoders
  - custom encoding algorithms
- People are mad so called PRIV8 shell → execution → fun in the end

OUTPUT

```
<Training>
  <TrainingItem>
    <title>Embed</title>
    <productType>Flash Authoring</productType>
    <trainingLink>http://www.adobe.com</trainingLink>
    <trainingLength>45+ Min</trainingLength>
    <trainingDesc>Using Testwerk software.
- Install Testwerk and configure it.</trainingDesc>
    <trainingLevel>Advanced</trainingLevel>
    <Recommended>False</Recommended>
    <rating>1</rating>
  </TrainingItem>
  <TrainingItem>
    <title>Web Services</title>
    <productType>Flash Authoring</productType>
    <trainingLink>http://www.adobe.com</trainingLink>
    <trainingLength>1 - 15 Min</trainingLength>
    <trainingDesc>Using AS3 Web Services in Flash.</trainingDesc>
    <trainingLevel>Basic</trainingLevel>
    <Recommended>True</Recommended>
    <rating>1</rating>
  </TrainingItem>
</Training>
```

Method #5

- Using a newly released book/learning material as base and infecting it
  - pdf exploit suite (search it ;)), swf infection or just plain old msf will do
- people want everything for free, but most of them uses many defensive tech still don't isolate their pdf reader

Method #6

- Open source projects from repos + magic code
  - How many of you actually read and understand the code ? Before executing ?
- Forking a project with added enhancements ;)
- Converting it into windows binaries → fun

Method #7

You Tell me!

Thank you

- am@hcon.in
- fb.com/root.hcon
- Twitter.com/HconSTF
- G+ AshishMistry