ACM Cyber

Kali Linux Tools

tinyurl.com/KaliToolsSlides

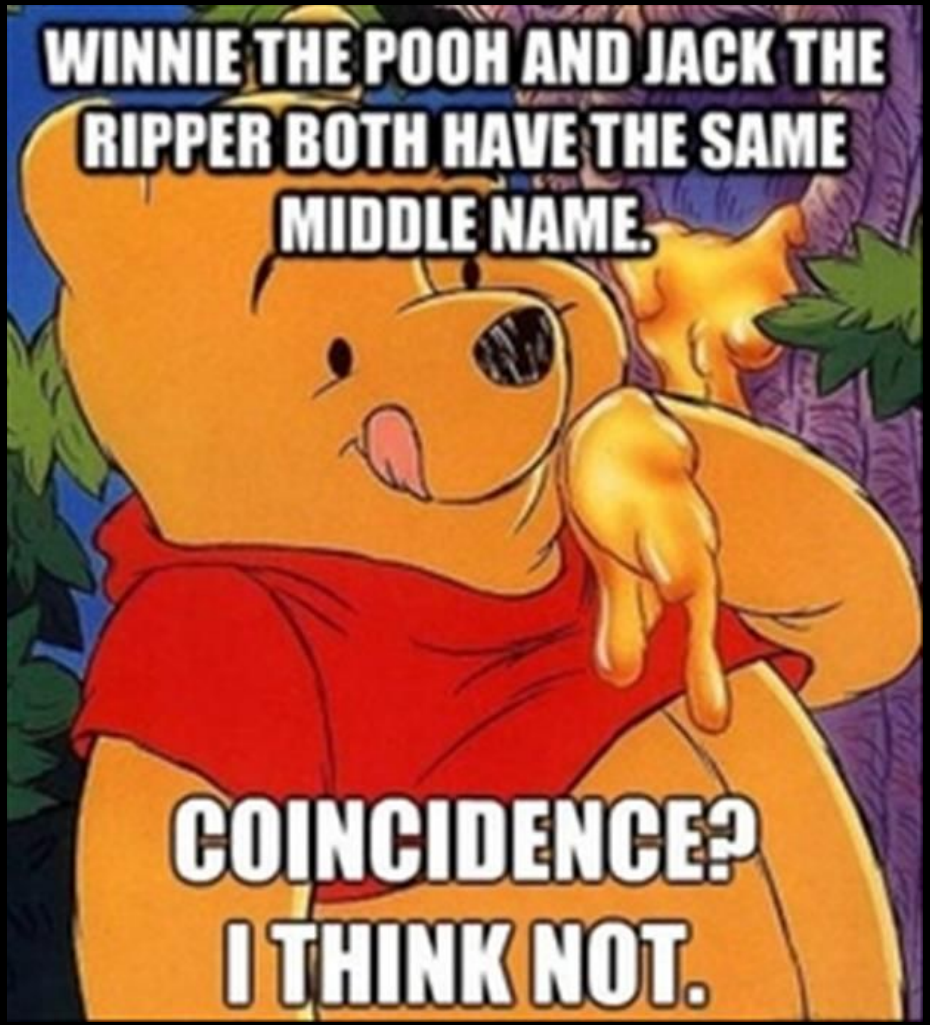
Overview

1) John the Ripper
    a) Hashes
    b) Passwords
    c) Password crackers
    d) Demo
    e) Challenge

2) Social Engineering Toolkit

John The Ripper

password cracker


WINNIE THE POOH AND JACK THE RIPPER BOTH HAVE THE SAME MIDDLE NAME.
COINCIDENCE?
I THINK NOT.

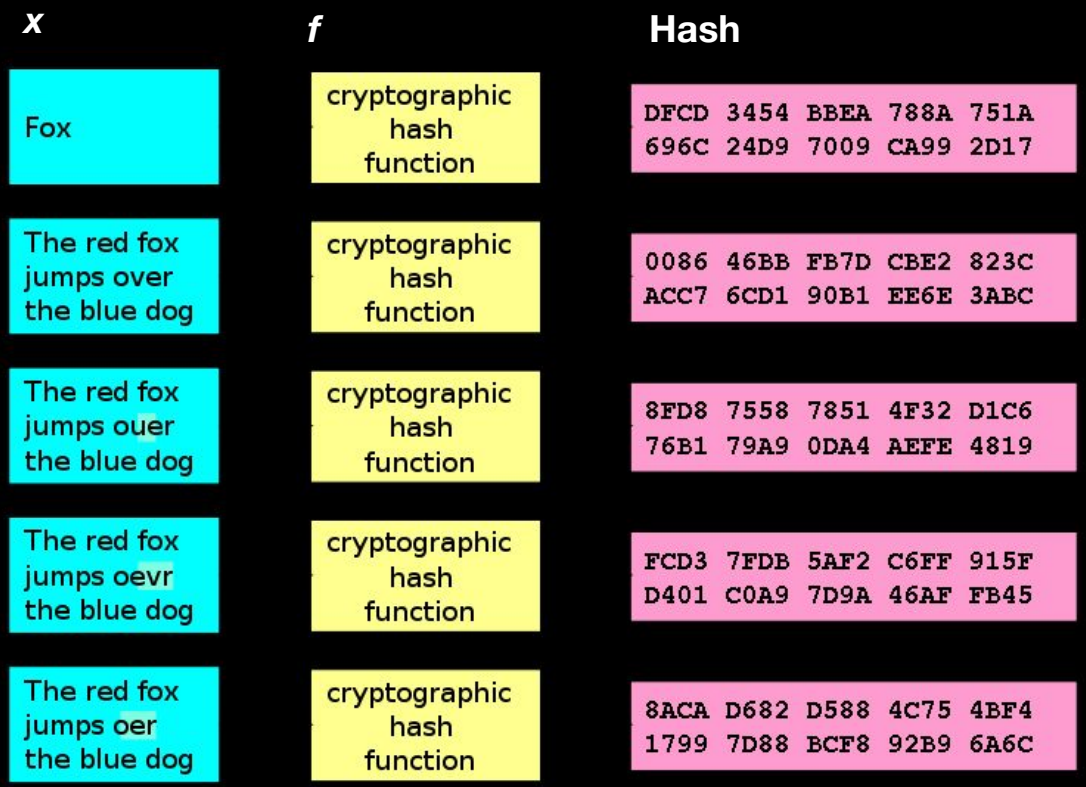
Hashes

“fingerprint” of some data

Hash function, *f(x)*

- Mathematical algorithm that maps data of arbitrary size to a string of a fixed size
- One-way function
- Easy to compute, f(x) but it is very difficult to compute their inverse function, $f^{-1}(x)$
- Or in other words, having data x, it is easy to calculate f(x) but, on the other hand, knowing the value of f(x) it is quite difficult to calculate the value of x
- Used to generate hashes

Hash, *f(x)*


x
f
Hash
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Popular Cryptographics Hash Functions

- MD5 (Message Digest)
    - Hashes that are 128 bits in length, expressed as 32 hexadecimal characters

- SHA (*Secure Hashing Algorithm*)
    - SHA-1 and SHA-256, which produce 160-bit and 256-bit hashes respectively (expressed as 40 and 64 characters)

Collisions?

Passwords

Passwords

- Passwords in secure systems (databases, OS) are usually stored as hashes

- Hash(“johntheripper123”) = 6541c37bb43c395de6e4872f1ba0977508b4db5be735129c45489b8f51999198

- When you try to login to a system with your password. The system takes your input and hashes it to get a hash *H1*. It then fetches the hash, *H0* of your password from a database. *If H1 == H2*, then you’re authenticated.

Passwords in databases

lol123	$2y$10$hV76dDIwwv3iTzOhik9EYuBcfbfQEzDU8DODJovvzUR...
admin	$2y$10$HKJSoPn6yAxbz6SKKPEogezyGEjQQ0/CX3e3ZqZOEvl...
hero	$2y$10$VA.5YMtTExSj6xixr1z6e.X/FqcYCZFRnAnCIM3RghW...

John The Ripper

John

- Password cracking tool written mostly in C
- Password cracking is a CPU-intensive and long process
- John offers multiple modes/methods to crack a password
    - Single crack/Guess mode
    - Wordlist/Brute force mode (/usr/share/john/password.lst)
    - Incremental mode
    - External mode
    - https://www.openwall.com/john/doc/MODES.shtml

Demo

write-up

Try out
https://www.hackthissite.org/playlevel/5/

Social Engineering Toolkit

Social Engineering Toolkit (SET)

Social Engineering Toolkit (SET)

- Social-Engineering Attacks >> Website Attack Vectors >>
  >> **Credential Harvester Attack Method >> site clone**
- **DNS Poisoning**

```
sudo setoolkit
```

Try out this problem!

https://gist.github.com/its-akshara/717ba1f9a33dc9298027fa7b15fef132

And this really hard problem!

https://gist.github.com/Sanjana-Sarda/8f1c4801591e3f666f98c3dd571c8f13

Thank you!

tinyurl.com/KaliToolsFeedback

Suggestions

- Math of RSA
- More External Resources
- More CTF Nights
- No Joe's Account
- Data Breach Breakdowns
- How to create a virus (Open Source Malware)