Introduction to hacking

Ian-Kyle Wagner

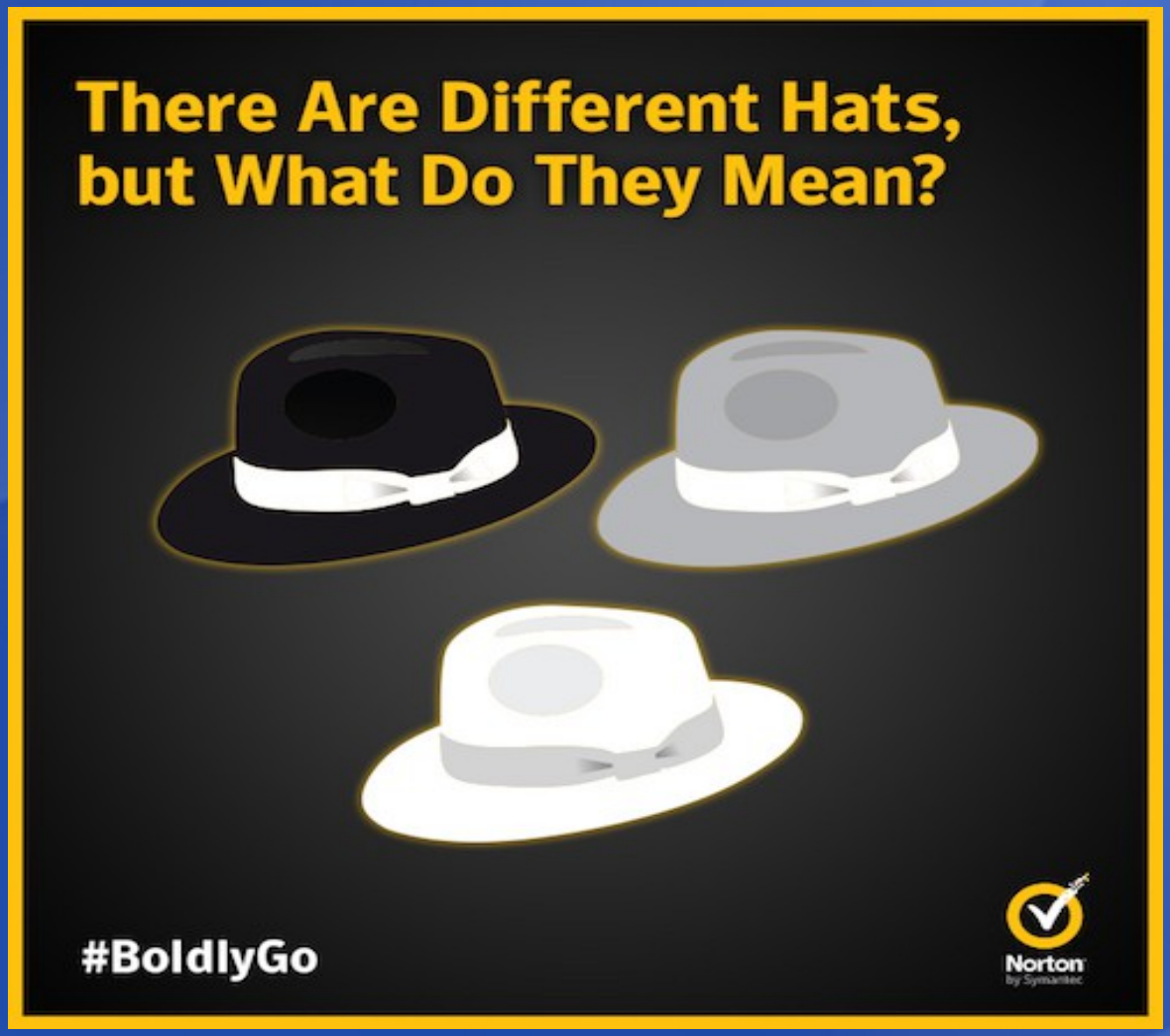
Table of contents

What is hacking

To gain access to a system through vulnerabilities such as buffer overflows, vulnerable SQL queries and etc.

Multiple hacking philosophies and levels

Hacker philosophies



http://community.norton.com/en/system/files/u2038063/what%20is%20the%20difference%20between%20white%20hat%20black%20hat%20grey%20hat%20hackers.jpg

Kali Linux

- Based off debian testing
- Latest software
- Preconfigured
- Live CD

http://distrowatch.com/images/cgfjoewdlbc/kali-small.png

Included tools

Examples:

https://images.duckduckgo.com/iu/?u=http%3A%2F%2F4.bp.blogspot.com%2F-vQeitQHGqNM%2FUEfCSNIHbzI%2FAAAAAAAABQg%2FL2UC4shMRMU%2Fs1600%2Fjohntheripper1_design.png&f=1

https://github.com/beefproject/beef/wiki

https://images.duckduckgo.com/iu/?u=https%3A%2F%2Ftse1.mm.bing.net%2Fth%3Fid%3DOIP.e2wqK893FFsUmtKtvyLV9QEsEs%26pid%3D15.1&f=1

Kali Linux install demonstration

512 MB mininum (RAM)
LXDE,XFCE

2048 MB for gnome shell

https://images.duckduckgo.com/iu/?u=https%3A%2F%2Fwww.deskmodder.de%2Fblog%2Fwp-content%2Fuploads%2F2013%2F08%2Fvirtualbox-logo-500x500.png&f=1

https://images.duckduckgo.com/iu/?u=http%3A%2F%2Fwww.laintimes.com%2Fwp-content%2Fuploads%2F2015%2F01%2Fvmware-logo.jpg&f=1

Introduction to hacking techniques

- Buffer overflow exploits (Metasploit)
- SQL injection
- Password cracking

Buffer overflows attacks

writes excess data to unassigned memory, causing an unexpected result

http://www.horstmann.com/sjsu/spring2008/cs40/buffer-overflow1.jpg

Buffer overflow continued

Unexpected behavior

Multiple factors:

Versions

Platform (OS)

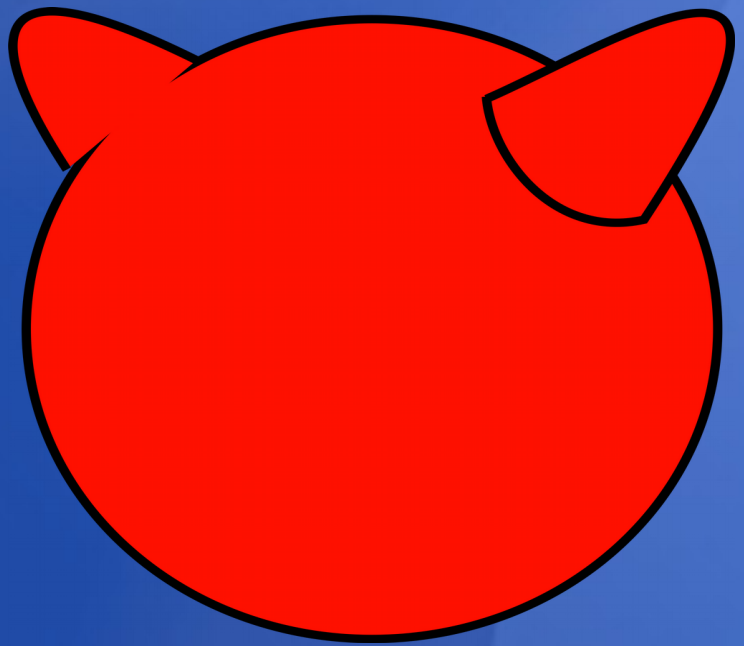
http://www.unixstickers.com/image/cache/data/stickers/C/C%20language.sh-600x600.png

http://www.unixstickers.com/image/cache/data/stickers/C/xC++-unofficial.sh-340x340.png.pagespeed.ic.wWgTbRiN5B.png

Buffer overflow example

Metasploit module telnet vulnerability

https://images.duckduckgo.com/iu/?u=http%3A%2F%2Fmybroadband.co.za%2Fnews%2Fwp-content%2Fuploads%2F2013%2F03%2FDigital-security-lock-encryption-cryptographic-keys.jpg&f=1



https://images.duckduckgo.com/iu/?u=https%3A%2F%2Fopenclipart.org%2Fimage%2F2400px%2Fsvg_to_png%2F204237%2FfreeBSD_2d_logo.png&f=1

SQL injections

Consists of injecting SQL code to gain unauthorized access through queries

SQL injections

Examples:

admin'--

admin” or “1=1”

1=1

...

Password cracking

Gain access from a compromised system

Ntlm, SHA1, etc.

https://images.duckduckgo.com/iu/?u=http%3A%2F%2F4.bp.blogspot.com%2F-vQeitQHGqNM%2FUEfCSNIHbzI%2FAAAAAAAABQg%2FL2UC4shMRMU%2Fs1600%2Fjohntheripper1_design.png&f=1

https://images.duckduckgo.com/iu/?u=http%3A%2F%2Fwww.welivesecurity.com%2Fwp-content%2Fuploads%2Fes-la%2F2013%2F09%2Fhashcat-logo.jpg&f=1

Cheat sheat:
http://pentestmonkey.net/cheat-sheet/john-the-ripper-hash-formats

Hacking tools demonstrated

https://images.duckduckgo.com/iu/?u=http%3A%2F%2F4.bp.blogspot.com%2F-vQeitQHGqNM%2FUEfCSNIHbzI%2FAAAAAAAABQg%2FL2UC4shMRMU%2Fs1600%2Fjohntheripper1_design.png&f=1

https://github.com/beefproject/beef/wiki

https://images.duckduckgo.com/iu/?u=https%3A%2F%2Ftse1.mm.bing.net%2Fth%3Fid%3DOIP.e2wqK893FFsUmtKtvyLV9QEsEs%26pid%3D15.1&f=1

https://images.duckduckgo.com/iu/?u=https%3A%2F%2Ftse4.mm.bing.net%2Fth%3Fid%3DOIP.M28aa9b75eaad0b6db34f88dbd05c9f2co0%26pid%3D15.1&f=1

Password hash cracking

Challenge MD5 hash

- 25f9e794323b453885f5181f1b624d0b
- Challenge SHA1 hash
- 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8

Metasploit exercice (Buffer overflow)

Try to hack the Windows XP virtual machine:

10.10.20.106 using the MS08-067 exploit

Goal is to display the victim using vnc (reverse tcp)

Recommended books

- The basics of hacking and penetration testing
- Hacking the art of exploitation
- Metasploit the penetration tester's guide
- Black hat python
- For more books:
- https://github.com/SpyVsCat5/Book-List

Where to go from here

Practice challenges (CTF):

Slack #ctf

Hacking club (proxmox)

https://ringzer0team.com/images/rz2.png

https://i.ytimg.com/vi/XKYkuDy_OIU/maxresdefault.jpg