

Forum:[Hack Forums](#)

Thread: [Free eBook WiFi Penetration Testing - A Practical Guide to WiFi and System Hacking](#)

virajnaik - May 9, 2017, 12:21 am

I am the author of WiFi Penetration Testing and I am offering it for Free eBook on amazon kindle for today.

Install Amazon Kindle to search & get WiFi Penetration Testing - A Practical Guide to WiFi and System Hacking eBook for Absolutely Free. Hurry!! Offer valid only for today.

Author: Viraj Naik

This book is designed to teach beginners and penetration testers who wants to have practical knowledge on how to hack or penetrate different things such as hacking WiFi, Facebook, Computers, Mobiles and so on using the tricks and techniques used by black hat hackers and professional penetration testers.

If you find it difficult to search in amazon and download then inbox me and I will send you the link to download.

This book comprises of seven chapters which are designed to make you a professional hacker in just a few days.

1. Introduction to Wireless Network:

This chapter is just the introduction to Wireless Networks and teaches you about the benefits and drawbacks of wireless networks, wireless modes, encryption, wireless antenna and so on.

2. Penetration Testing Lab Setup:

This chapter is designed to assist you to setup your penetration testing lab and practice all exercises included in this book. In this section, you will learn about hardware and software requirement for setting up penetration testing lab, creating bootable medias, using a virtual environment, wireless adapters, basics about the command line, configure routers and network interfaces, working with files, directories, managing software, word-lists and so on.

3. Hacking Wireless Networks:

In hacking wireless networks, you will be able to learn about how you can perform different types of wireless attacks, which you can use to crack WEP, WPA, WPA2, exploit WPS feature, hacking when network is busy, hacking idle network, hacking a wireless network with no clients connected, perform Denial of service address, reveal hidden SSID, bypassing MAC filtering and much more.

4. Evil Twin and Fake Access Point:

This chapter teaches you about how you can set up a rogue access point and evil twin network to perform different types of sniffing and man in the middle attacks on the wireless clients.

5. Information Gathering and Scanning:

In this chapter, you will be able to learn how you can determine a list of hosts which are live, their MAC addresses, open ports, services running, OS, different types of scanning techniques, identifying security vulnerabilities in the network and systems and so on.

6. Sniffing:

In this chapter, you will be able to learn about how you can successfully perform sniffing, its types, perform arp spoofing, sniffing Facebook passwords, MAC flooding, DHCP starvation and rogue DHCP server, DNS poisoning and much more.

7. Exploitation:

Exploitation is the last and the most exciting chapter in this book. In this, you will be able to learn about hacking wireless client via discovered vulnerabilities, using Metasploit framework, generating Trojans, offering fake updates to the clients, hacking android device and so on.

pomwtin - May 9, 2017, 1:54 am

Well I had some spare time and I made a bit of a review:

1) Kali and VMware- You should tell reader NOT TO install kali in VMware with actual ISO, but use VMware image instead- a lot of issues are avoided this way.

2) Good job on quick linux intro (explanation of basic commands) and some AP settings.

3) Generating "X in length numeric.. etc etc" wordlists in crunch is USELESS WASTE OF HDD- you should not encourage such actions in your book- such dictionaries are best generated on-the-fly

4) Starting monitor mode creates you wlan0mon -> after this you kill it with mon0... I am kind of getting a feeling that you just put together random resources found online ?

5) in airodump description- not a word about RXQ- the MOST IMPORTANT value

6) Again.. wlan0mon.. mon0... wlan0mon... mon0.. this can be confusing to a reader

7) On page 29 and 32 and 36.... you are actually capturing data from AP from which you lose 92% and 89% and 93%.... of packets (useless capture -> misleading to reader) RXQ value meaning!

8) WPS section- not a word about pixie dust- you really need to look this one up

9) Page 58- finally capturing from AP where 0% packet miss occurs :)

10) --ignore-negative-one just hides the message you know...

11) Cracking WPA.. with aircrack- not best option; with RAINBOWTABLES- you have to be joking- ESSID is included in hashing process, therefore it is useless to use them. Direct brute force is a way to go, but you are saying to reader to first generate rainbow table and then use it on handshake.. this will cost reader twice more of time.

12) DUDE- NOT A WORD ABOUT HASHCAT

13) I like the post-exploitation chapter, gives reader a bit of an insight what can be done

14) OK THIS ONE REALLY GETS ME- YOU CLEARED YOUR CACHE, THEREFORE YOU WERE ABLE TO BYPASS HSTS FOR FACEBOOK DOMAIN AND GAINED PASSWORD USING DNS SPOOFING- NOT A SINGLE WORD ABOUT WHAT WAS NEEDED TO DO TO ACHIEVE THIS. WITHOUT HSTS BYPASS IN ONE WAY OR ANOTHER THIS ATTACK WOULD FAIL- MISLEADING OF A READER ONCE AGAIN (i wrote it with capslock on on purpose)

This would be it..

Honestly, You left me with a feeling that you are not really sure what you were doing most of the time, also your knowledge about cracking does not appear to be good enough to write a book about it.

I hope I did not anger you in one way or another... this is a truly honest review

EDIT: I just noted you are supposed to have CEH v8... maybe you should re-take it ?

darilay25 - May 9, 2017, 11:46 am

hi, i can't pm you Due To a new account can you send me the link?

virajnaik - May 9, 2017, 10:49 pm

(May 9, 2017 11:46 AM)darilay25 Wrote: [\[CITE\]](#) hi, i can't pm you Due To a new account can you send me the link?

Free Promotion got over. You can search for "WiFi Penetration Testing - A practical guide to WiFi and System Hacking in Amazon to download.

Diditdyan - May 22, 2017, 11:12 am

Give me the link please, i cant PM you thx

Numinous - May 22, 2017, 11:13 am

can i get this one ?

thank you

Capt. Murphy - May 26, 2017, 4:22 pm

(May 9, 2017 01:54 AM)pomwtin Wrote: [\[CITE\]](#) Well I had some spare time and I made a bit of a review:

1) Kali and VMware- You should tell reader NOT TO install kali in VMware with actual ISO, but use VMware image instead- a lot of issues are avoided this way.

2) Good job on quick linux intro (explanation of basic commands) and some AP settings.

3) Generating "X in length numeric.. etc etc" wordlists in crunch is USELESS WASTE OF HDD- you should not encourage such actions in your book- such ductionaries are best generated on-the-fly

4) Starting monitor mode creates you wlan0mon -> after this you kill it with mon0... I am kind of getting a feeling that you just put together random resources found online ?

5) in airodump description- not a word about RXQ- the MOST IMPORTANT value

6) Again.. wlan0mon.. mon0... wlan0mon... mon0.. this can be confusing to a reader

7) On page 29 and 32 and 36.... you are actually capturing data from AP from wich you loose 92% and 89% and 93%.... of packets (useless capture -> missleading to reader) RXQ value meaning!

8) WPS section- not a word about pixie dust- you really need to look this one up

9) Page 58- finnaly capturing from AP where 0% packet miss occurs :)

10) --ignore-negative-one just hides the message you know...

11) Cracking WPA.. with aircrack- not best option; with RAINBOWTABLES- you have to be joking- ESSID is included in hashing process, therefor it is useless to use them. Direct bruteforce is a way to go, but you are saying to reader to first generate rainbowtable and then use it on handshake.. this will cost reader twice more of time.

12) DUDE- NOT A WORD ABOUT HASHCAT

13) I like the post-explotation chapter, gives reader a bit of an insight what can be done

14) OK THIS ONE REALLY GETS ME- YOU CLEARED YOUR CACHE, THEREFOR YOU WERE ABLE TO BYPASS HSTS FOR FACEBOOK DOMAIN AND GAINED PASWORD USING DNS SPOOFING- NOT A SINGLE WORD ABOUT WHAT WAS NEEDED TO DO TO ACHEIVE THIS. WITHOUT HSTS BYPASS IN ONE WAY OR ANOTHER THIS ATTACK WOULD FAIL- MISSLEADING OF A READER ONCE AGAIN (i wrote it with capslock on on purpose)

This would be it..

Honestly, You left me with a feeling that you are not really sure what you were doing most of the time, also your knowledge about cracking does not appear to be good enough to write a book about

it.

I hope I did not anger you in one way or another... this is a truly honest review

EDIT: I just noted you are supposed to have CEH v8... maybe you should re-take it ?

Damn! When the pros come rolling in, LOL!!! He shouldn't be offended but take your advice and level up his game. If this is an offense, dude is in the wrong line of work. That's doing it for the ego, and that gets you locked up or gets someone's system f'ed up (assuming one is a real penetration tester, not a hobbyist for bragging rights <EGO>)...

zask - May 27, 2017, 1:26 pm

Could you trade me it for one of my books

Ghostzapper - May 28, 2017, 6:28 am

Wow, sounds like powmtin is the real pro here. It would be great if he wrote an ebook. Now that would be helpful to the rest of us. Also if it's ok with him, his review of the book should be posted on Amazon so that this charlatan doesn't make money with his fake ebook which he is obviously pushing. Unfortunately, he seems to have come to the wrong place to flaunt his "expertise".

Anubis - May 28, 2017, 3:38 pm

Please send me this book. I need it for my research. Thanks.

Jacob5263 - May 28, 2017, 9:49 pm

thanks needed to learn how to do this

DamnHari97 - May 30, 2017, 1:04 am

Can u send me the link for downloading the ebook

R A B B - June 1, 2017, 8:58 am

Would like the ebook. I already know wifi crackin

Most of my neighborhood I can drive around no problem ne hotspotted haha.

But love the reads

CreativeHold - July 23, 2018, 4:11 pm

I'll take a copy please. Thanks in advance