

Forum:[Hack Forums](#)

Thread: [Wireless Penetration Testing and Security \[From Beginner to a WiFi Pentesting Ninja\]](#)

rootsh3ll - August 17, 2017, 3:38 am

The most practical and comprehensive WiFi Penetration testing guide in the world.

This eBook features 10 chapters, over 30,000 words, and lots of interesting WiFi hacking attack vectors that are nowhere on the internet—all designed to deliver you a comprehensive and unparalleled Wireless penetration testing education—along a support forum.

Whether you're an intermediate in need of new strategies and a good wireless attack vector, or you're just getting started in penetration testing with wireless networks—you're in the right place.

In This eBook, You Will Learn:

How to install Kali Linux

Let's start at the very beginning. In this chapter, we'll settle on our practice lab, Install Kali Linux on Virtual machine and HDD both. This chapter will get you started thinking about what is Kali Linux, how to configure your wireless lab, and how to accomplish most out of it in terms of WiFi pentesting with plenty of images to help you at every step.

[Click here](#) for demo

How to Crack Wireless Network Security

From the uses you may know of some tools that we use during wireless pentests, we'll cover what penetration testers (like at DefCon) are doing with tools today. Included here are many best practices and suggestions for how to not get stuck when a tool stops working, while exploring the variety of ways to hack the wireless security like WPA/2 and WPS manually.

[Click here](#) to learn more

Post Exploiting the Network

In this chapter, we demystify the process of post exploitation of machines over the LAN and sniffing the traffic and analysing it with packet analyser. Whether you identify as a penetration tester or a beginner, completely inept in both facets, we've got you covered with tons of step-by-step advice and resources that will help you become a ninja WiFi hacker. Not to mention you also get free 3-months subscription forums.

[Click here](#) for demo

What is a Rogue Access Point

Once you've created the copy of your target access point, party has just begun. In this chapter, we'll discuss some common Access Point spoofing strategies and speak in layman's terms about what it really means to test your fake access points. Leave the coding and stuff at home, and we'll talk common sense strategies for better and best working rogue access points.

[Click here](#) for demo

Captive Portals: Exploiting Android/iOS Devices

You can design and create the best net in the ocean, but if you're not near the fish, you'll never catch a thing. The same goes for your access points. If your landing page doesn't have a stealthy and trustworthy mechanism to pwn this victim, it doesn't have power to give you the most out of your setup and attack strategy. And no victim, means no information breach. We'll discuss no-nonsense methods you can use to create the automatic popup splash screen that you see instantly when connected to public WiFi like Starbucks, and how to hack Android/iOS device with it on automation.

Hacking Cleartext WiFi Passwords, No Gimmicks

Once you've got all the setup working, and victims coming into your honeypot, it's time to wonder what's next. We'll take you beyond the world of traditional fake access point that's ever been taught in this chapter, and discuss some super powerful and out-of-the-box automation tactics, to give you an idea of what you can do with your fake access point. TL;DR few folks did perform this attack at DefCon this Year to sniff cleartext WiFi passwords.

[Click here](#) to learn more

Simultaneous Single Adapter AP(s) + Client

It is not difficult to assume that during wireless pentesting people do end up having only one Wi-Fi NIC and struggle to crack into the target wireless network sometimes, thanks to WPA2. In this chapter, we learn how to create virtual interfaces on a single adapter and run multiple access point while connected to personal hotspot with same card, simultaneously. Connectify for Linux? Yes, we are crafting our own here. Free of cost

Spoof Internet Access to Victim

If you are familiar with Fake access points, you might be having troubles with targeted rogue AP attack. A rogue AP with single adapter usually lacks no connection to WAN. Even if you create virtual interface, there is a chance you don't have an active Internet source. Hence, no Internet for client which can cause serious suspicion and cause client to disconnect from your fake access point. Here we learn to spoof the client (Windows, Android, iOS, Macintosh) to trick them and prevent automatic disconnection

You Might Be Wondering...

Is that all? what is special about this?

That's just the cream on the milk. There is so much more useful and in-depth content in the book and coming on the rootsh3ll forums that I can't wait to share it all with you. Like free webinars, updated scripts and attack vectors, video support, and so much more...

What if I get stuck?

We've got your back! We created a comprehensive resource to be valuable for beginners and pentesting veterans alike. Whether you need tips, tricks, or need to clear doubts, hop onto rootsh3ll forums and we assure to help you out.

Can I download this guide and read it later?

We're glad you asked! You sure can. As soon as you make the purchase, the PDF version of this course is sent to you so that can download it (3 times at max), print it, share it with colleagues, and read it at your leisure.

Can I start leaning WiFi hacking right now?

By all means! In fact, I'd love that. Check out this page to get started with WiFi hacking right away. As you read The Ultimate Guide to WiFi hacking, you can build your own attacks with the information you learn.

Having troubles with the payment? [Try this](#)

Keep Learning
-Harry

Quentin Coldwater - August 20, 2017, 7:43 am

Looks promising. Hope you will have nice sells you know your stuff :)

Kareem - August 20, 2017, 8:07 am

PM me for some thread tips since I like your product! GLWS

rootsh3ll - August 20, 2017, 8:52 am

(Aug 20, 2017 07:43 AM)Quentin Coldwater Wrote: [\[CITE\]](#) Looks promising. Hope you will have nice sells you know your stuff :)Thanks Quentin. You can always mail me on harry@rootsh3ll.com for your queries :)

Quentin Coldwater - August 23, 2017, 12:18 pm

Just keeping thread alive. Might be worth it

rootsh3ll - August 24, 2017, 5:37 am

(Aug 23, 2017 12:18 PM)Quentin Coldwater Wrote: [\[CITE\]](#) Just keeping thread alive. Might be worth it
Thanks Quentin.

:)

hopeforme - August 24, 2017, 6:31 am

I'm an ultra beginner and I'm interested in your book. Would like someone to rate it though.

Temp_reassign - August 24, 2017, 7:03 am

Why do I feel like I should buy this? Any chance I can get a preview of how the tut is laid out? Going by your thread alone, its worth a buy but...

BTW, GoodLuck

rootsh3ll - August 24, 2017, 11:43 am

(Aug 24, 2017 06:31 AM)hopeforme Wrote: [\[CITE\]](#) I'm an ultra beginner and I'm interested in your book. Would like someone to rate it though.

Thanks for showing interest. eBook is currently hosted on my site. You can make your [purchase here](#) and if you have any issues with PayPal, you can try this link as well: <https://gum.co/klwps>

About rating: That'd be really helpful. Can you help me with that? I have no idea how to do it ?

(Aug 24, 2017 07:03 AM)Temp_reassign Wrote: [\[CITE\]](#) Why do I feel like I should buy this? Any chance I can get a preview of how the tut is laid out? Going by your thread alone, its worth a buy but...

BTW, GoodLuck

I would suggest you won't regret going with your feeling this time ?

I have included links to the tutorials (though they ain't that good looking as in book but it's good enough for idea) you notice the "Click here for demo" under few Blue sections ? click on it to see the demo.

Though I am putting those links here as well for future readers. Here it goes:

How to install Kali Linux

<https://rootsh3ll.com/rwsps-installing-and-configuring-kali-linux-ch1pt1/>

How to Crack Wireless Network Security

<https://rootsh3ll.com/rwsps-wpa2-cracking-aircrack-ng-dictionary-attack-ch3pt4/>

Post Exploiting the Network

<https://rootsh3ll.com/rwsps-post-exploiting-the-network-ch6/>

What is a Rogue Access Point

<https://rootsh3ll.com/fake-wifi-access-point-walkthrough/>

Hacking Cleartext WiFi Passwords, No Gimmicks

<https://rootsh3ll.com/ultimate-fake-access-point-walkthrough/>

Thanks for GL :)