UNDER THE HOODIE:
ASK A PENETRATION TESTER

If you could ask a pen tester anything about the dark art of pen testing, what would you ask?

We asked our customers to submit their questions to Rapid7 pen tester Leon Johnson, and they didn't hold back. From "What's in your go-to toolkit?" to "What is your go-to song while performing a pen test?" we have Leon's answer. Read below for a glimpse into the inner-thinking of a hired hacker. ►►►

Well, I've been a pen tester but I switched from red to blue almost 6 years ago. In recent years, what has been the most effective avenue of attack?

LEON: It's almost always passwords that are the downfall of networks. While the points of entry may change, you will no doubt have been using MS08-067. Also probably taking advantage of default passwords on things like tomcat and Databases. Once you are in, the attacks become the same.

We have been doing more network attacks, such as LLMNR, DNS, NetBIOS, etc. These are not new but are being attacked more frequently, likely because the tools to attack them are getting better. I think that's what drives most attacks: the tools.

With professional pen testing being saturated with "varying levels of talent" over the past decade; how do you differentiate yourself in a meaningful way?

LEON: It's important to confirm and meet the client's needs. Sometimes clients are confused about the value that certain offerings provide, or have purchased an engagement that doesn't actually suit their need. The first thing we instill in our consultants is to provide exceptional customer service and to understand and deliver upon what is most important to their clients.

Secondly, we match our clients up with the consultants best suited to their unique needs. For example, when we identify a network that might pose a special challenge, we will assign someone who is already familiar with that kind of environment. (Or I will go! Ha.)

Rapid7 puts an emphasis on internal and external training. We have created a lot of internal content to help our fellow pen testers learn from each other's' experiences. Most recently, we have made some of this content externally available through Rapid7's training classes: www.rapid7.com/training-certification.

What does it feel like when you pwn a system?

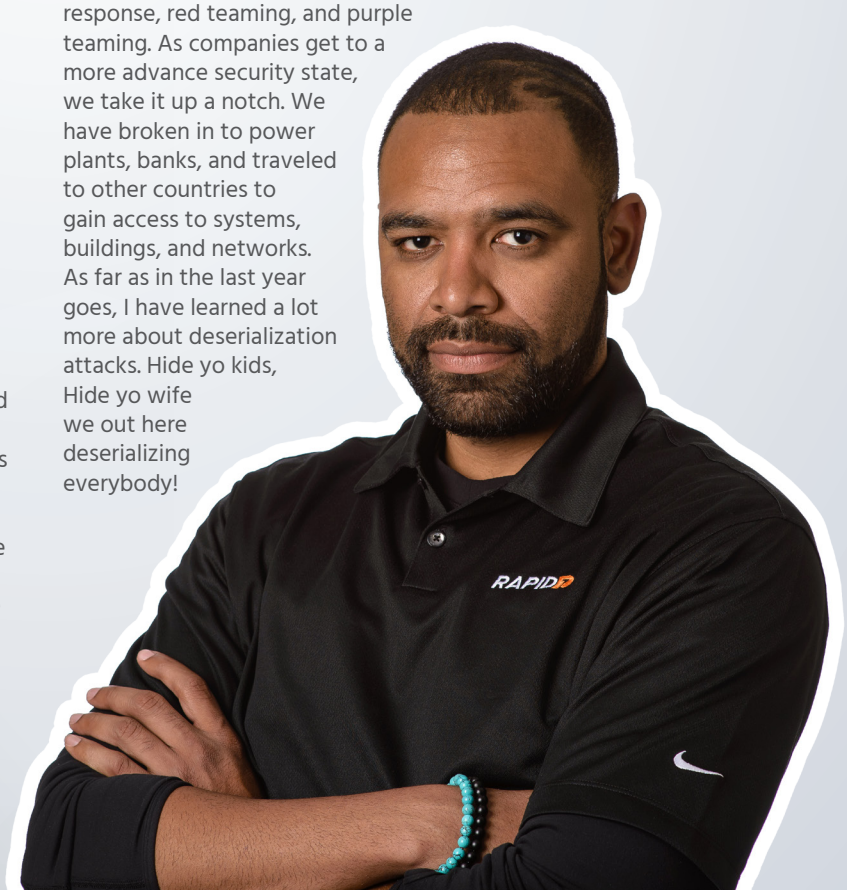
LEON: It never gets old, I'll tell you that!! Since I have been doing this for quite a while, I get most excited when I hear about new ways. I would estimate that in 75% of the assessments I see, the attacks are somewhat the same.

What is the most important quality/trait that a pen tester could have that would make him/her successful?

LEON: At the risk of you being some sort of all-powerful being set out to remove all of my skills except for the one I choose, I would say perseverance. ;)

As companies evolve (ideally) it becomes more difficult to achieve the goals of a pen test. What new skill(s) have you had to learn in the last year to stay competitive?

LEON: I've become much more experienced with incident response, red teaming, and purple teaming. As companies get to a more advance security state, we take it up a notch. We have broken in to power plants, banks, and traveled to other countries to gain access to systems, buildings, and networks. As far as in the last year goes, I have learned a lot more about deserialization attacks. Hide yo kids, Hide yo wife we out here deserializing everybody!



Leon Johnson
Rapid7 pen tester

> I would estimate that in 75% of the assessments I see, the attacks are somewhat the same.

What have you found to be the most effective way to crack a perimeter? Phishing seems likely to top the list, but are there other classes of vulnerabilities that have consistently worked well or that are particularly common?

LEON: While phishing will always provide some sort of attack vector, I have also had success with physical access and any non-two factor remote logins including OWA, VPNs, content managers, and really any logins.

How does it feel when you finally are at the shell of a system - must be a thrill?

LEON: Same answer as Pwn system. However, you would be surprised at how easy it sometimes is. Once I compromised an application on the kick off call because they had a database with default credentials on the Internet. Yeah…. don't do that.

What's in your go-to toolkit?

LEON: No one tool will get you all the way there, and almost every tool will fail you at some point so it's important to have multiple ways of doing things. I like to tell my clients that if I have Metasploit open you are probably in a lot of trouble. ;) I also use Crackmapexec, Impacket, Responder, Powershell Empire, and Mana wireless. Rapid7 also has a lot of tools that we have created, some of which are available at https://github.com/MooseDojo.

How do you stay current with all the research being published?

LEON: I have found that I learn something new on almost every assessment I complete. I figure out what puzzle is ahead of me, do research on that specific puzzle, and then become current on any attacks I don't already know about the environment. Unfortunately, many environments require only fundamental attacks to be successful.

What industry related book are you reading now?

LEON: The Car Hacker's Handbook: A Guide for the Penetration Tester, and blogs and twitter. Twitter is like the news for vulnerabilities and new hacks.

Do you use a distro like Kali or do you roll your own?

LEON: Both, however I mostly use Kali because I'm lazy! Kali is nice because it has nearly everything all ready to go.

What is your overall process for performing a penetration test in regards to client-side vs. Web application vs network?

LEON: Lately I have been taking advantage of macros in Excel spreadsheets. I pretext clients well enough to get them to click on something and/or do something.

If all phishing was prohibited from the scope of a pen test what would be your approach to breach the perimeter?

LEON: Look for OWA first and do reconnaissance. Examine what services are externally facing the web - applications, logins, services. Determine the username structure. Guess passwords. Look for database-driven applications that might not be secured.

I know the scope of a pen test must be defined in an agreement, but can't the limit of the scope give a false sense of security? I mean, if a system that is not part of the scope would actually open a path to other systems included in the scope, the results wouldn't quite correspond to the reality.

This is something that we explain to all our clients.

What was your most memorable pen test?

LEON: I once performed a penetration test in five different countries. I flew to China, Dubai, Korea, Russia, and Greece performing internal assessments and social engineering.

Have you ever went out of scope on a penetration test to prove something to a client?

LEON: Only with the client's permission!

How often do you need to write your own tools vs. use existing tools?

LEON: You can get by almost exclusively using existing tools, however when I need to I bust out my magnificent coding skills.

What methods do you use for cataloguing tools that you've written, queries that you've found useful, etc. so you don't have to figure it out again the next time you run into a situation where they are useful?

LEON: Sad but true answer: I have a txt file. I also use GitHub and leverage an internal Rapid7 pen test team wiki that's always growing.

When do you decide enough is enough testing when performing a penetration test?

LEON: That depends on the goals of the assessment. Often times this is a discussion with the client. When they yell mercy. Only if they yell it though. ;)

What is your go to song while performing a pen test?

LEON: I listen to lounge music. I used to listen to SomaFM but now I make my own playlist with online music players that allow me to download the music.

When performing a pen test against a mobile application, what are your methodology differences vs. Testing a website?

LEON: I spend more time looking at how the application interacts with the host with phone vs web. Data storage for mobile applications seems to be less vetted vs web applications.

What's the average length of your pen tests? What is the ideal length? What's the longest pen test you've ever been on? The shortest?

LEON: Ideal length is debatable - we often go with one week, however it all depends on the goal and size of the assessment. I once did a five week assessment in five different countries, and another time I spent three weeks in one building doing multiple tests. The shortest test I've done was one day.

What's the number one thing a company can do to thwart a pen tester?

LEON: We need to define thwart first. That being said I will go with Segmentation. Segmentation! Final answer.

What resources do you recommend for becoming adept at pen testing?

LEON: YouTube, Twitter, challenges boxes like VulnHub, CTF's, "Hacking Exposed" books, and Rapid7's training courses (look up the Rapid7 Assault Courses). I also recommend that you build out a lab and play - hack your own box!

Other than a laptop, what gear do you bring with you on a pen test?

LEON: A bootable usb, routers, wireless cards, teensy device, lock picks, lan turtle hak5, portable wireless devices 4G, and my personality.

How important is it to be fluent in a scripting language on the average pen test?

LEON: You don't necessarily have to know how to program or script. However if you do, you can move more quickly, and that makes you much more efficient!

How much time do you actually spending performing the pen test vs other related activities (scoping, contract negotiations, report writing, etc.).

LEON: As a penetration tester at Rapid7, it should be at least 75% of your time. Report writing takes up most of the remaining time, with research to fill any gaps.

What's the most creative defense that's you've discovered during a pen test?

LEON: Broken networks, where I have to fix it to hack it! Also networks, where even though you are in the office, you have to vpn to use anything. It's harder to hack those.

How do you protect the business information that you exploit during the test?

LEON: We encrypt all information and then wipe the data once reporting is complete.

From your experience, if you had to design a secure application, what secure coding strategies would you recommend?

LEON: That's a good question! I would implement mandatory security training for developers so they can proactively identify and address vulnerabilities, implement security testing within the development lifecycle, and hire an in-house security team to perform testing.

Get more under the Under the Hoodie insights at
www.rapid7.com/info/under-the-hoodie.

Do you want to see if Leon or one of our other esteemed penetration testers from Rapid7 can get into your network? Learn about our Penetration Testing Services at www.rapid7.com/pentest