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're back for another round of pen tester Q&A. This time, Jesse Gardner fielded the questions from our customers, covering everything from Active Directory assessments to IoT pen testing. Read below for a look behind the curtain with a hired hacker. ▸▸▸

What framework, methods, or tools do you recommend for O365 penetration testing?

JESSE: Office 365 (O365) presents some unique challenges for penetration testing, but there aren't any O365-specific frameworks or tools that come to mind. Examples of tools you can use to test O365/Exchange mail and other mail systems: Metasploit, MailSniper, Empire, PowerSploit, Unicorn, etc. with some of the more exciting exploits being those around 2FA and MDM bypasses. Once you get access to O365, start hunting for sensitive info or resources and begin pivoting from there.

How do you recommend preparing for a pen test with Amazon Web Servers and/or Google Cloud?

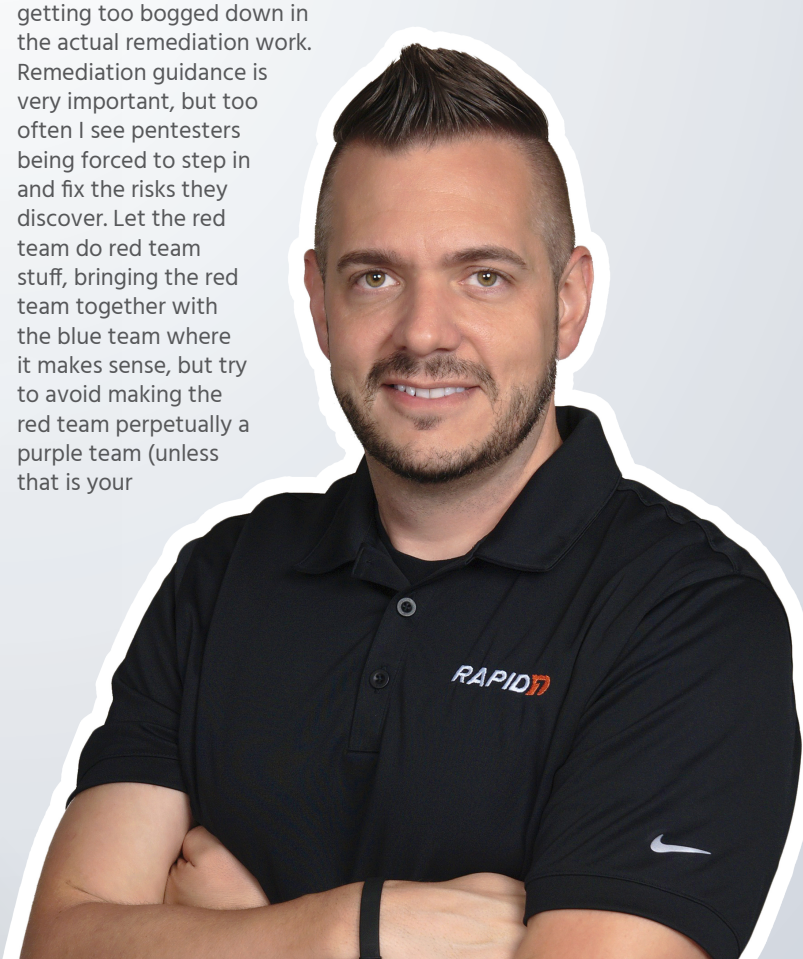
JESSE: Some service providers require prior notification of penetration testing exercises (i.e. AWS requires a request authorization form be filled out, Google Cloud does not), so you'll want to abide by your business partner's terms, but those logistics aside, it really depends on the environment. For example, sometimes we test cloud instances from within a customer's virtual private cloud (VPC), where our customer will spin up an instance for us to use during testing that resides with or very near other target cloud instances. Other times we treat those cloud targets like any other externally-facing target, using specific engagement objectives to guide us to whichever threat modeling best suits our customer's needs. Discussing your environment and topology early in the assessment scoping process will really help to set things up for a successful engagement.

Where do you see pentesting evolving over the next 10 - 20 years, specifically with regard to Artifictual Intelligence and Machine Learning?

JESSE: Offensive tools will continue to grow in complexity and breadth. That said, I could see greater automation occurring as a form of AI, where the logic behind that automation is fueled by machine learning. Part of the trick to this is a greater understanding of the environment(s) being reviewed and meaningful comparison across a large set of baselines. Penetration testing difficulties for AI and machine learning lie in the complexity and uniqueness of targets, where humans can draw upon experiential logic and intuition faster than our silicon counterparts. I think it is inevitable that improvements will be seen in the coming years that take advantage of sewing together machine learning and AI for what we do.

How should an organization approach the creation of their own internal pentesting methodology?

JESSE: It's great when an organization tackles pentesting internally; it can go a long way toward cross-team education about organizationally-shared risks and vulnerabilities. Methodology-wise, I would recommend working hard to keep the pentesting team focused on assessments and prevent them from getting too bogged down in the actual remediation work. Remediation guidance is very important, but too often I see pentesters being forced to step in and fix the risks they discover. Let the red team do red team stuff, bringing the red team together with the blue team where it makes sense, but try to avoid making the red team perpetually a purple team (unless that is your



Jesse Gardner
Rapid7 pen tester

> Regardless of an organization's maturity in their own digital transformation process, penetration testing and security review is a crucial component in that transformation.

overall goal). One more tip: as you are building team hierarchy, watch out for ego issues when traversing interdepartmental boundaries, nobody wants to hear that their baby is ugly, so that part can take some real finesse — make sure your stakeholders are champions in diplomacy.

What are the 10 best pentesting tools for AD assessment?

JESSE: Here are 10 goodies (in no particular order):

- Metasploit msfconsole (oodles and oodles of AD-specific modules)
- Nmap / Masscan (to scan all the things)
- DNSRecon / Fierce (find targets in DNS - Zone Transfers, PTR lookups, etc.)
- Responder.py (various Man-in-the-Middle and relay attacks)
- CrackMapExec (excellent post-exploitation tool, especially for large environments)
- Empire (PowerShell post-exploitation framework)
- PowerSploit (PowerShell post-exploitation framework)
- BloodHound (""Six Degrees of Domain Admin"")
- httpscreenshot / EyeWitness (to discover and review web services)
- ADExplorer (great for AD object reconnaissance and searching)

How has your approach changed since the last "ask a pentester"?

JESSE: I would say that holistically our approach hasn't changed much. Our pentesting team and services offerings have grown a lot in the last year, and with that growth we've been formalizing our tactics, techniques and procedures towards certain verticals or technologies. But overall, those refinements in our approach are felt more at the micro level than the macro level.

What are your thoughts on pentesting as part of the digital transformation process?

JESSE: Regardless of an organization's maturity in their own digital transformation process, penetration testing and security review is a crucial component in that transformation. The sooner security-focused stakeholders and business partners are involved in this process, the easier it is to "bake in" security to that ecosystem, services or products. As they say: an ounce of prevention is worth a pound of cure. Periodic and ongoing security review/testing is a must, especially during technological change.

Do you participate in bug bounties? How does that influence your day job?

JESSE: Personally, I don't participate in any bug bounties. Like most, I have a lot of infosec interests and hobbies vying for my attention at any given moment, but I do have some colleagues that manage to squeeze in the occasional bounty time. Of those friends that participate in bug bounties, it seems to me that they do it more for fun and for honing a particular skill or attack chain, than to get rich from bounties. I would say the same about CTFs, as I have several friends that are very active in the CTF scene.

From your experience what is the best advice you would give to an upcoming analyst regarding certifications?

JESSE: Some people love certifications and some people hate them. Certifications have merit, and can be a gateway drug to more certifications, an exciting first step into a new career field, or an opened door to new job opportunities. I think it is great to go after certifications to increase your knowledge and credentials, but would caveat that it must be done with humility. I have worked with some really amazing professionals that didn't sprinkle alphabet soup in their signature block, as well as some cert junkies that struggle to summon the vast powers of certification when they need it most. Looking back on similar discussions I've had with folks, I can't think of a time I didn't persuade them to charge after the certification they had their eye on. As we like to say: Hack all the things!!!

What are the best tools for pentesting SAP applications?

JESSE: There are a few tools out there (even some SAP-specific modules in Metasploit), but I would say a foundational and fundamental understanding of SAP systems and architecture is the most valuable tool in testing SAP. SAP systems can be complex and there are quite a few configuration and system management pitfalls that can be readily exploited. Furthermore, as with most applications, underlying host vulnerabilities or other common attacks such as authentication attacks can also be a factor. SAP is one of those systems where we have a few SAP gurus on the team that we lean on during these tests. I'm not guru status with SAP, but I know it is a challenging group of applications to protect and we often discover ancient SAP systems lingering in dark corners of people's infrastructure, underscoring the need to keep it up-to-date and regularly reviewed.

What are the best report-writing techniques you use?

JESSE: If I had to prioritize my report writing approach into a few key elements, they would be these: 1) Put myself in the shoes of those reading the report. I would want clear, concise explanations and guidance. I don't want a full display of hacker fu technojargon showboating, as cool as that can be sometimes. 2) Be meticulous in details, but not at the expense of readability. If the risk is

not well explained or the proof of concept and guidance is not well articulated, you better believe the exposure will not be understood, or even worse, it will be left unaddressed. I like my reporting like I like my logging: -vvv mode, but I also throw in some -h to make it human-readable. 3) Stringent peer review. As I'm writing reports, I know that fellow pentesters will be scrutinizing my work to challenge my methods and catch my mistakes. This is as much a relief as it is a motivating factor to do my very best, and it provides a great way to share tactics, techniques, and procedures with one another.

What is your pentesting approach towards ICS scada attacks?

JESSE: Industrial Control System (ICS) or supervisory control and data acquisition (SCADA) testing is something we carry out from time to time, and in several different forms. Sometimes ICS/SCADA is the target of testing, or we bump up against these systems on internal network testing, or we perform testing on embedded devices related to ICS/SCADA. Special care and consideration needs to be taken in testing these targets, as adverse effects could have far reaching real world implications. Whenever we're testing ICS/SCADA targets, we work closely with our customer to make sure the goals of testing and any particulars about the target are well understood and defined. We approach these systems much like we approach any other system, but we devote more focus and attention to a few of these factors: system isolation, protocols in use, Man-in-the-Middle or replay attacks, management systems, etc.

Please discuss your reporting process. How much is template-driven? How much do you write from scratch? Do you use any particular tools to write your reports?

JESSE: At a high level, our reports follow a straightforward outline with risk summaries, detailed and technical explanations of testing and/or attacks performed, as well as individual finding details. Each finding includes a summary of the identified risk, a detailed proof of concept with reproduceable steps, remediation guidance, and applicable references. Each individual report skeleton template is created using a customized version of the open source tool Serpico (SimplE RePort wrIting and CollaboratiOn tool). Using Serpico we have captured many common findings to help speed up the reporting process, but findings in Serpico are primarily place holders for us to flesh out with the engagement-specific finding details. If there isn't a template finding in Serpico, we insert a placeholder to write one from scratch — I can't recall a single report that didn't have some custom-written findings. Once we've captured all the findings in Serpico, we'll generate a Word document and begin writing. After a draft report is finished, it goes through a peer review process where other penetration testers review our work. Afterwards, the report goes to tech writers to get a final polish before being delivered to the customer.

What do you find most rewarding/challenging/exciting: internal or external pen tests ?

JESSE: I can recollect quite a few fun and frustrating times from both! I would say that internal pentests offer the most variety as far as targets go, but both can be rewarding, challenging, and exciting. Subjectively speaking, I think the most rewarding part of any pentest is when we pull off a hard-earned righteous, mind-blowing hack where we even surprise ourselves. Some of the most challenging times are when we go after a really difficult target while the customer is tracking our every move and they burn all our shells. But sometimes those assessments can quickly turn into an exciting and rewarding test once we get that magic foothold. One of the beautiful things about this job is that we never know what we are going to get. Sometimes we are forced to rely on pure tenacity and intravenous Red Bull.

How is pentesting as a bug bounty program? Should organizations adopt a bug bounty program? If so, can a bug bounty program be used in lieu of a pentesting program?

JESSE: It really depends on a lot of different factors, such as the types of systems you're looking to protect, the maturity of your cyber security processes, procedures, and staff, compliance obligations or obligations to business partners, and the types of threats you want to defend against, just to name a few. I think bounties and other types of vulnerability disclosure programs can be a powerful tool in hardening your systems, processes, and procedures, but I don't believe they fully replace the need for a traditional penetration testing regimen. There are several large organizations that use bug bounty programs, and when done right, they provide real value for the right use cases.

What has been the most effective attack you've seen in 2018?

JESSE: That is a tough one... there are so many good answers. For me personally, qualitatively I'd say OSINT information gathering and/or infrastructure reconnaissance that led to exposures in services or endpoints that led to exploitation in one form another. I try to not leave any stone unturned. More broadly, I'm still surprised to see the team frequently and consistently gaining footholds across various systems through password guessing attacks for all kinds of services. Shout out to our new old friend "Summer2018!".

What was your shortest pen test? (i.e. what was the shortest period of time it took to reach your goal?)

JESSE: For many of our penetration tests, we will work toward multiple discrete goals or broad objectives over the course of days or weeks. That being the case, it isn't unheard of for us smash through goals to get to the "crown jewels" within hours (or sometimes minutes) of starting our assessment. But we strive to go beyond the flash in the pan of getting Domain Admin access, to dig deeper and find those really scary risks and attack paths that your security staff loses sleep over. We don't stop searching/testing until we hit the end of the assessment timeframe.

Have you ever gotten in trouble with a customer or even worse, law enforcement, over a pen test engagement that went sideways?

JESSE: There have certainly been precarious situations. As you might imagine, we often push the limits of systems, controls, and personnel. Knock on wood, I have not been in any tangles with law enforcement during an engagement yet. The threat of police involvement has been very real, especially on physical and social engineering penetration tests. We cover a lot of the "what if" and worst case scenarios with our customers prior to testing, so we are pretty well prepared for surprises and have middle-of-the-night points of contact. There have been situations where teammates have had to explain themselves to law enforcement, usually due to a lapse in communication with local personnel at a facility, but nobody was detained. I have a running joke with some friends who always ask me if I've been pepper sprayed or tased yet, maybe one day the answer will be "yes", but not yet.

What is your approach to IoT pentesting?

JESSE: An effective IoT testing methodology should consider the entire solution, or as we refer to it, the IoT Product Ecosystem. This could include but is not limited to:

- Embedded devices and associated physical components sensors, receivers, and actuators
- Control software such as mobile applications or thick clients
- Cloud APIs and associated web services
- Network communication protocols (Ethernet, 802.11 WiFi, etc.)
- Intra-component communication such as Bluetooth, Zigbee, Z-Wave, etc.
- Failure of any component of the product ecosystem can and will affect IoT security posture. Only through a thorough examination of the entire ecosystem can you holistically test the security of IoT targets.

Are there public IRC/Slack etc. or groups that you've found invaluable for picking up new tricks from members or friends?

JESSE: My Slack client has 9 teams in it right now, I'm pretty active in 3 or so, but might hit 1 or 2 of the others on occasion, with several of them being a private group of friends. Chances are good that there is a Slack team for tools or groups you might have interest in, bloodhoundhq.slack.com is a good example. I'd suggest asking around, some of the Slack teams I've joined were mentioned via Twitter by the teams running them. I haven't really been active on IRC for a couple of years or so (sometimes I consider revisiting some old haunts) but I guess you could say I rely primarily on Twitter, Slack, and Reddit for relevant news and discussions.

Is there any framework for pentesting?

JESSE: There are several security testing methodologies and frameworks out there, a few that come to mind are PTES, OWASP, and ATT&CK. To complement any framework, there are quite a few security and best practice guidance consortiums and resources such as NIST, DISA STIGs, CIS Benchmarks, SANS CIS CSCs, etc. They all have their focuses and strengths so I would recommend diving into as much information as you can get your hands on to determine which guidance and practices most closely align with the technologies and systems you're trying to protect. At Rapid7 we've been focusing on NIST guidance for our penetration testing services but we often align with and include relevant guidance and recommendations from many other reputable sources.

How do you ensure that Rapid7 is providing a unified experience for engagements? Do you utilize a playbook of some sort?

JESSE: We have a lot of shared tactics, techniques, and procedures that the team has built and refined over the years. That said, I believe the closeness of our team is probably the biggest factor in maintaining unified continuity in our practices. We pride ourselves on our organization's culture, we communicate well and often, we meet regularly for team hackathons where we're able to share techniques and new tools or methods (much like a mini security conference), and we are all very passionate about what we do. This makes it easier to share methods or critique one another's work during peer reviews for the betterment of the team. We love what we do!

.....

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.