John Richardson

Candidate – Information Security Analyst

ACC Security Responses

1. Security can be summed up into two mindsets, the breaker and the fixer. Which one are you?
   1. I also believe there is a third mindset, the breaker/fixer, or the Purple Hat, who comfortably crosses over from either area. For a person to be a good security analyst, the best person is the one who understands both sides of the ‘firewall,’ irrespective of wearing the Black Hat or the White Hat. I do enjoy the ‘breaker’ role, performing the passive and active pen tests but then taking that knowledge and mitigating the findings. At the same time, it is also fun, probably more so, to play the Blue Team and work to block the hacker. To limit oneself to only Breaking or Fixing, is to be crippled in being able to truly protect the network and systems.
2. How would you build the ultimate botnet?
   1. There are a couple of ways using Kali Linux
      1. Register a domain with a similar name, e.g. goog1e.com
      2. Using Metasploit, copy some domain like Google and copy the files to the newly registered domain
      3. Embed a script on the site to open a Reverse\_TCP\_Shell
      4. Using Metasploit SET, create a phisher email to send with a link to the ‘neutral’ site, using something similar to “Click here for Nude Photos of Jennifer Lawrence” or you can create a payload and deliver it in the email disguised as a PDF or some other ‘innocent’ file
      5. Using theharvester on Kali Linux, harvest a group of emails from sites such as Facebook, Google, etc.
      6. Connect to a non-logging VPN in some country such as Switzerland, Russia, etc.
      7. Use Nmap to determine an open SMTP server (port 25) that does not have RELAY turned off
      8. Distribute the phisher email via the relay SMTP server
      9. Wait for the Reverse\_TCP\_Shell and once connected, quickly start a service such as NOTEPAD.EXE and overwrite the file and run it as SYSTEM
   2. Using BeEF
      1. Open up BeEF
      2. Copy the DEMO PAGE link from the application
      3. Using a public IP address, modify the DEMO PAGE link in BeEF to include the routable IP address
      4. Using a fake YouTube account for posting, find a video that gets lots of hits and post a comment that piques the curiosity of the viewer and add the URL to the comment, such as “Click here to find out how to hack Facebook passwords”
      5. Those who click on the link with then be part of your BeEF Botnet.
   3. Or, if you want to go the easy route, you can connect to a VPN like above and then download an “Off the Shelf” application such as IceIX, UFONET, or LOIC and use that.
3. Argue 3 points why the end user is not the weakest link.
   1. The biggest reason that end users cannot be considered the weakest link is because surveys have proven that the majority of end users aren’t aware of Acceptable Use Policies (if there even is such a policy in place) or the company does not have Computer Safety training, one of the KEY components of an effective, mature security program. The company is failing to ensure end-users are properly trained and knowledgeable of best security practices
   2. Another reason end users aren’t the weakest link is that many companies do not invest in certain tools like an IPS, effective NextGen Application monitoring firewalls, etc.
   3. A third reason is that often times developers and operations (or DevOps) either incorrectly code an application for use but not security or software may be deployed with default username/passwords, not securely locked down like a SQL SA account with a blank password, etc.
4. What is worse in Firewall Detection, a false negative or a false positive? And Why?
   1. The more dangerous of the two is a False Negative because the firewall has allowed a bad actor into the network without any notification to staff or any SIEM.
5. Name 10 SIEM use cases
   1. To centralize event logging for active review and action
   2. To monitor the internal/external network traffic for any type of vulnerability scanner, such as OWASP ZAP, wpscan, or sqlmap
   3. To determine is a single account is being used concurrently from multiple systems at the same or very nearly same time that is abnormal for that user
   4. To monitor login points, such as VPN connection from a location that is not expected, e.g. North Korea
   5. To monitor for Intrusion detections, malware, viruses, etc.
   6. Monitor for system changes such as user account create/delete/modify, system modifications, etc.
   7. Statistical analysis for metrics such as IDS or IPS notifications, concurrent connections, etc.
   8. To monitor for Data Loss, large outbound FTP connection traffic, etc.
   9. To monitor for Session activities such as duration, who, etc.
   10. Monitor for abnormal administrative activities such as unchanged passwords, inactive accounts, etc.
   11. Connection details such as country of origin, entry point method such as VPN, etc.
6. What is residual risk? Name residual risk in your life.
   1. Residual risk is that amount of risk remaining after mitigation steps have been taken, such as a firewall, IPS, HIPS, anti-malware, etc. have been deployed but still systems are still powered on and connected to a network which means there is still a small amount of risk such as a Zero-Day phisher, or a USB-delivered key logger tool that can be used to infiltrate the network. An example of a risk in my or anyone’s life is evidenced in needing to have auto insurance. We can have lane departure warnings, air bags, modulating speed control radar, seat belts, etc. and yet we still have auto insurance to defer the remaining risk of a drunk driver.
7. What is the most interesting incident you worked on? Describe it as detailed as possible.
   1. One of the more interesting incidents came several years ago while I was working at Texas Windstorm Insurance Association. We had a user who kept complaining of being kicked off the network, he would reboot and then be fine for a while. After checking his DHCP, I found that the addressed assigned was not APIPA or the defined scope for his VLAN. Finally, I deployed Wireshark, captured his traffic and found his address was being assigned by a rogue DHCP server. Finding the IP of the rogue DHCP server, I made an HTTP connection and found it was a D-Link router. The hunt was then on. Walking around all cubicles, I quickly found a small home router that a contractor had brought in because he wanted two drops in his cubicle and had not cleared it with IT nor had he turned off the DHCP option. We removed the router and the issue was resolved. IT Management was engaged and they determined there was no intentional malevolent purpose and merely instructed him to not do that again.
8. What is your approach to implementing a new security event manager?
   1. Talk to the stakeholders and determine the need of the business.
   2. Perform the risk gap analysis to determine current state and what is missing
   3. Research the products available using a scorecard to determine the product that meets the most needs
   4. Read the whitepapers, watch the marketing and available training videos of the top 3 products
   5. Speak with technical pre-sales to ask any specific questions of pain points, examples of metrics, etc.
   6. Work towards a POC
   7. Have staff trained on selected tool
   8. Provide Cost Benefit Analysis
   9. Deploy the product in the learning phases and try to have a week or more of learning time to help dial down the False alerts and actively continue to monitor for false negatives
   10. Get feedback from business of any potential impact to workflow and address accordingly
   11. Make live in production and have an up to one month period of continuing to closely and actively monitor the tool
9. How do you learn? Hands on, book, audio, something else?
   1. I learn best with a combination of methods to help reinforce the lesson. I’m fine with books and do read quite a bit as well as watch numerous YouTube videos, vendor videos, etc. However, I also have my lab at home where I get hands on with the tools, Kali, CISCO routers and switches, etc. which is ideal for me. Then, the third is not dissimilar to a back and forth discourse with peers.
10. You are given 500 pieces of straw and told that 1 piece is a needle which looks like straw. How would you find the needle? What other pieces of information would you like to have?
    1. My initial search is to acquire a magnet and run the magnet over, around, and through the pile of straw and allow the magnet to pick up the needle.
    2. A second method would be to take the straw individually and perform a slight bend and the one that gives the most resistance would be the suspect.
    3. A third option is to burn the straw and the one that does not burn is the needle but that to me is the worst option since it destroys everything around it. If this search is to find the intruder in the network, then if everything is destroyed, what are you trying to save?
11. What was the most interesting thing you found in Vault 7
    1. If I found one thing most interesting in the hack it is the vast amount of materials that were hacked and released, materials that should have been so secure but that have been compromised. As far as data, I really didn’t find much in Vault 7 that was earth shattering. The fact that code was released and not simply “Hey, we can do this, this, and this” was probably the most intriguing. However, all in all, it was more of a confirmation of rumors that already abound, that TVs can be used in Recon, that the CIA is active in hacking, that the government can hack Apple, Windows, and Android phones, that the government has worked with Microsoft and others to build back doors and to get crypto keys, etc.