Why leave PRT?

Currently because PRT is very new, most of our work involves tuning of process, much less technical than when I was explained in the interview process. An example would be emailing vendors asking for technical recommendations. Pace is also quite slow; I'm not getting enough work as I hoped for. All in all, I feel like I'm not growing enough in this role that I'm in, so I asked FX if I could transfer into AA instead.

General:

1. **What are TTPs?**
    - **Tactics, Techniques, and Procedures** (TTPs) describe the behavioral patterns used by threat actors to achieve their objectives. An example would be the following: a common tactic an attacker might employ is evasion. The technique used could be process injection via process hollowing. The procedure would be to drop a DLL which would sideload with a process like MS teams
    - Upon running would:
        1. Create a new suspended svchost process (CreateProcessA)
        2. Zero out (NtUnmapViewOfSection)
        3. Alloc rwx memory (VirtualAllocEx)
        4. Unsuspend the process.
2. **Dictionary Attack vs Bruteforce vs Rainbow table.**
    - A Dictionary Attack is using common words or default passwords. Bruteforce is when you use different permutation of inputs, like 1111, 1112, 1113. Rainbow table attack is when you compare a hash input with a precomputed table of hashes.
3. **What is Pass-the-hash Attack?**
    - In a Windows environment, an NTLM hash is treated equally as a plaintext equivalent. As such, an attacker can authenticate to a resource by providing the NTLM hash without cracking it.
4. **What is Port Scanning?**
    - Port Scanning checks open ports on a networked device, helping identify services running on a system and potential vulnerabilities that might be exploited.
5. **What is a Sniffing Attack?**
    - In a Sniffing Attack, an attacker intercepts and monitors network traffic to capture sensitive data such as login credentials.
6. **Explain Phishing.**

- Phishing is a social engineering attack where attackers trick individuals into revealing sensitive information by posing as trustworthy entities, often via emails or fake websites.

7. **Explain Spear Phishing.**
    - Spear Phishing is a targeted form of phishing that tailors messages to specific individuals, making them appear more credible and increasing the likelihood of success.
8. **Explain Whaling.**
    - Whaling targets high-profile individuals, like executives, with customized phishing attacks to gain access to sensitive information or resources.
9. **Explain Vishing.**
    - Vishing (voice phishing) is a form of phishing that uses voice calls to manipulate individuals into providing sensitive information.
10. **What is an Exploit and Payload?**
    - An **exploit** is code or software used to take advantage of a vulnerability. The **payload** is the part of the exploit that performs malicious actions, such as installing malware.
11. **What is Spoofing?**
    - Spoofing is the act of disguising oneself as another entity to deceive systems or individuals, such as email or IP address spoofing.
12. **Explain DOS and DDOS Attack.**
    - **DoS (Denial-of-Service)** attacks disrupt services by overwhelming them with traffic. **DDoS (Distributed Denial-of-Service)** uses multiple systems to amplify the attack.
13. **Explain SYN Flood Attack.**
    - A SYN Flood sends a series of SYN requests to a server without completing the handshake, overloading the server and potentially causing it to crash.
14. **Explain ARP Poisoning.**
    - ARP Poisoning manipulates ARP tables on a network to intercept or disrupt traffic by falsely associating an attacker's MAC address with an IP address.
15. **Explain MITM Attack.**
    - A Man-in-the-Middle (MITM) Attack intercepts communication between two parties, allowing attackers to eavesdrop or alter data.
16. **Explain DNS Poisoning.**
    - DNS Poisoning, or DNS spoofing, involves altering DNS records to redirect users to malicious websites without their knowledge.
17. **What is DNS Tunneling?**

- DNS Tunneling uses DNS protocol to communicate with malicious servers, often for data exfiltration or command-and-control in attacks.

18. **What is a Drive-by-download?**
    - A Drive-by-download automatically installs malware on a user's system simply by visiting a compromised or malicious website.
19. **What is Malware?**
    - Malware is software specifically designed to harm, exploit, or otherwise negatively impact systems, networks, or data.
20. **Explain Different Types of Malware.**
    - Types include **viruses**, **worms**, **trojans**, **ransomware**, **spyware**, and **adware**.
21. **Difference between Virus, Trojan, and Worm?**
    - **Virus:** Attaches to files and spreads when executed.
      Trojan: Disguised as legitimate software but performs malicious actions.
      Worm: Self-replicating malware that spreads across networks.
22. **What is Fileless Malware?**
    - Fileless Malware operates in memory without creating files on disk, making it harder to detect by traditional antivirus software.
23. **What is OWASP?**
    - The Open Web Application Security Project (OWASP) is a nonprofit organization dedicated to improving software security through open-source projects, including the OWASP Top 10.
24. **Explain SQL Injection.**
    - SQL Injection is an attack where an attacker inserts malicious SQL statements into a query, enabling unauthorized access to a database.
25. **Explain Cross Site Scripting (XSS).**
    - XSS is a vulnerability that allows attackers to inject malicious scripts into webpages, affecting users who visit the page.
26. **Explain Cross Site Request Forgery (CSRF).**
    - CSRF tricks a user into performing actions they didn't intend, often by exploiting their authenticated session with a website.
27. **Explain Broken Authentication.**
    - Broken Authentication refers to vulnerabilities that allow attackers to bypass authentication and assume the identities of other users.

28. **Explain Broken Access Control.**
    - Broken Access Control occurs when users gain unauthorized access to restricted resources or actions.
29. **How do you keep yourself updated with information security?**
    - I stay updated by following security blogs, participating in online communities, and attending relevant conferences and training.
30. **What are Black Hat, White Hat, and Gray Hat?**
    - **Black Hat**: Hackers with malicious intent.
      White Hat: Ethical hackers who help secure systems.
      Gray Hat: Hackers who may use legal or illegal means but have neutral or mixed motives.
31. **Do you know any programming language?**
    - Yes, I am familiar with languages like [Python, JavaScript, etc.]. (Specify your known languages.)
32. **How can you define Blue Team and Red Team?**
    - **Red Team** simulates attacks to test defenses, while the **Blue Team** defends the system against real and simulated attacks.
33. **What is a Firewall?**
    - A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on security rules.
34. **Explain Security Misconfiguration.**
    - Security misconfiguration refers to insecure settings or default configurations, leaving systems vulnerable to attacks.
35. **Explain Vulnerability, Risk, and Threat.**
    - **Vulnerability**: Weakness in a system.
      Risk: Likelihood of a vulnerability being exploited.
      Threat: Potential cause of an unwanted incident.
36. **What is Compliance?**
    - Compliance involves adhering to laws, regulations, and standards to ensure security and privacy practices meet certain criteria.
37. **What is MITRE ATT&CK?**
    - MITRE ATT&CK is a knowledge base of adversary tactics and techniques, helping organizations understand and defend against cyber threats.
38. **Do you have any project that we can look at?**

- Yes, I have worked on [describe relevant project], which focuses on [focus of project, e.g., threat detection, vulnerability scanning].

39. **Explain 2FA.**
    - Two-Factor Authentication (2FA) requires two verification methods to access an account, providing additional security.
40. **Could you share some general endpoint security product names?**
    - Examples include Symantec Endpoint Protection, McAfee, and CrowdStrike.
41. **What are HIDS and NIDS?**
    - **HIDS (Host-Based Intrusion Detection System)**: Monitors a single device.
      NIDS (Network-Based Intrusion Detection System): Monitors network traffic for suspicious activity.
42. **What is the CIA Triad?**
    - **Confidentiality, Integrity, and Availability (CIA)**: The core principles of information security.
43. **What is AAA?**
    - **Authentication, Authorization, and Accounting**: Framework for controlling access and tracking activity.
44. **What is Cyber Kill Chain?**
    - The Cyber Kill Chain is a framework that outlines the stages of a cyberattack from reconnaissance to execution.
45. **What is SIEM?**
    - **Security Information and Event Management (SIEM)** consolidates security data, providing real-time analysis and alerts.
46. **What is Indicator of Compromise (IOC)?**
    - IOCs are evidence or data points indicating potential malicious activity within a network.
47. **What is Indicator of Attack (IOA)?**
    - IOAs identify the intent behind actions that may indicate an attack, regardless of compromise.
48. **Explain True Positive and False Positive.**
    - **True Positive**: Correct detection of a threat.
      False Positive: Incorrectly identifying non-malicious activity as a threat.
49. In the case of a directory traversal, if an attacker attempts to access a resource such as win.ini, we can correlate this attempt with HTTP response codes, if available HTTP

response body and windows event logs 4663 to check if the file was indeed accessed. If the response code is 200, and there was a successful object access windows event log, this will be indicative of a true positive.

50. For command injection, we can look at windows event logs 4688 for process creation and if there was a successful attempt to spawn a new process.
51. For data exfiltration