Connor Schuler
SEC-250-02
STR2026

1. A US Government research laboratory has just developed a new radar technology that makes modern stealth aircraft, no longer stealthy. The radar can operate in the presence of jammers and tests show that it effectively detects all modern stealth aircraft on 99% of the encounters. The project is still in a developmental stage, there is little documentation on the system. Hardware designs, logic schematics and software are all stored on a cluster of computers in the research lab which is defended by two firewalls, and intrusion detection system and all of the data is encrypted based on the users login key. The research lab is located on a Naval Base in Maryland access is restricted.

The most likely attackers for this scenario is a nationstate hacker or a corporate spy. This kind of military technology would be a massive gain for any of the US's many enemies or nations of interest. Additionally, if it was a contract based development, other companies might be interested in stealing the plans and getting a new contract.

If I was an attacker, I would attempt an inside attack or social engineering attack. It would be the simplest way to infiltrate the computer systems, since a direct attack would almost certainly be detected. I would look to target employees who could be compromised such as outside contractors, and target times when they should be firmly between cybersecurity training and least on the lookout for phishing attempts.

To protect against this I would do thorough background checks and extensive cybersecurity training.

2. A small company that designs leading edge network monitoring and management software with a customer base of tens of thousands including most of the Fortune 500 and many government agencies. The software operates on customer networks with privileges. The companies code base is stored on secured servers inside a secure building with strong access controls in place.

The most likely attackers for this scenario are a corporate spy or a cybercriminal. Other companies would be very interested in the technology/data and access that this company could have. On the other hand, cybercriminals could see it as an opportunity to compromise thousands of companies and extort them via ransomware.

In terms of attack methods, I would use a direct network attack or social engineering attack. It would be the simplest way to infiltrate their computer systems, there is almost certainly a web portal or other internal service that could be compromised. I would look to target employees who could be compromised such as outside contractors, and target times when they should be firmly between cybersecurity training and least on the lookout for phishing attempts.

To protect against this I would install thorough network security, intrusion detection systems, and conduct extensive cybersecurity training.