Whitney Carpenter

CSCI 452

Dr. Lin

1/25/26

The Deceptive Heart and the Trusted Network: A Reflection on Jeremiah 17:9 in Network Penetration Testing

Introduction

Network penetration testing is a discipline that starts from the assumption that systems and users cannot be trusted at face value. We can actually apply biblical truth to this assumption as well. Jeremiah 17:9 tells us, "the heart is deceitful above all things, and desperately sick; who can understand it?" This verse shows the unreliability of apparent trust, since deception isn't always obvious; sometimes it comes from within. Network penetration testing is not just something we do technically; it is an ethical responsibility backed up by core human beliefs. Throughout this essay, I will examine how this biblical passage of Jeremiah 17:9 guides us in engaging ethically with network penetration testing, based on the verse's direct parallels to the core assumptions, methodologies, and ethical responsibilities involved in the process.

Deception and False Trust in Networks

In the past, enterprise networks heavily relied on implicit trust once a user or device was authenticated. This was very dangerous, as the perimeter was protected by firewalls, but the internal segmentation was weak, which allowed for lateral movement. This could also have the potential to lead to Trojan horses, where malicious programs disguise themselves as legitimate software. This is a direct comparison to Jeremiah 17:9. What everyone might assume is safe and trustworthy, the heart/trojan, was actually deceptive and could contain deeper corruption.

Now, penetration testers have the responsibility of protecting a system by assuming compromise even in "secure" environments. It is essential to always assume compromise is possible because internal users could act maliciously or negligently, and even if all of your users and devices are safe, credentials could still be stolen or abused. Verizon DBIR shows that credential misuse and insider-related access are still dominant attack vectors, proving that authentication does not equal trust (Verizon Business, 2024). Just as God tells us in Jeremiah, trust must be continuously questioned, because nothing is ever 100% secure.

Revealing Hidden Truths

A big part of penetration can be described as revealing hidden truths. Penetration testers' job is to uncover anything that routine monitoring misses. There are four phases of penetration testing: planning, discovery, attack, and reporting (Scarfone et al., 2008). After planning and setting the testing goals, the testers discover vulnerabilities, which they then attack and exploit. If the attack is successful, they will document the vulnerability as well as safeguards to mitigate the problem, and if the exploit ends up enabling testers to escalate their privileges on the system or network, additional testing is done before the documentation and reporting phase (Scarfone et al., 2008). Through this process, many hidden truths can be revealed, including silent misconfigurations such as excessive Active Directory permissions, hidden attack paths that enable lateral movement, or accumulated technical debt in legacy systems. Any one of these things could be detrimental to an organization, but without penetration testing to reveal them, they would continue to fester underneath the service, causing more damage.

We can see the comparison here to Jeremiah 17:9 as well. We cannot judge a system by what we see on the surface, since we now know how many things could be hidden underneath. Similarly, surface-level-judgement is not accurate against humans. Just like networks and

systems, humans could be functioning totally normally on the outside, even though they are fundamentally insecure or broken on the inside. When we feel this way, we know that we have to examine our hearts and take a deeper look inside to know what is going on. That is exactly what we are doing with penetration testing. We are revealing hidden truths, exposing realities that had been concealed underneath functional operations.

Human Factors and Insider Risk

Though it may not seem like it with the rising intensity of cyber threats, a whopping 68% of breaches involved a human element (Verizon Business, 2024). These human factors mostly consist of phishing, credential theft, and misuse of access, according to Verizon's Business Report (2024). The concept of self-deception that we see in Jeremiah 17:9 can be seen in human factors in risk like weak passwords, policy violations, and susceptibility to social engineering. We as humans often believe that our own behaviour is safe or insignificant when we're actually unintentionally creating attack vectors through these weak safeguards or vulnerabilities.

Furthermore, there are two types of insider risk. Some insider risk is malicious, meaning the user intentionally misuses their access, while some is unintentional, where mistakes are made or negligence plays a role. As Jeremiah 17:9 emphasizes, humans are not perfect. Even if it is an accident or a mistake, users must be considered untrustworthy for the system or network to be safe. Penetration testing must account for human fallibility, not just system vulnerabilities.

Ethical Responsibilities

Penetration testers have a big ethical responsibility on their shoulders, since they hold a lot of power by intentionally bypassing controls and accessing sensitive systems. The National Institute of Standards and Technology puts a big emphasis on the ethical responsibilities in

penetration testing. In the planning phase, rules of engagement are established that give the testers only the authorities and permissions they need, the scope is defined, making sure they don't penetrate anything that is not necessary, and then, when they are actually testing, it is controlled so as to avoid unintended harm (Scarfone et al., 2008).

It is important to recognize here that the testers are admitting that deception applies to themselves as well, not just others. That is exactly what Jeremiah 17:9 is trying to teach us: that we have to question ourselves because even our own hearts are deceitful. This awareness and mindset help to constrain tester authority, prevent exploitation beyond scope, and encourage honest and accurate reporting. Penetration testing requires humility and a heart and mind for service.

Application to Zero Trust Architecture

Zero Trust Architecture is essentially a formal rejection of implicit trust in networks. The core principles of Zero Trust are never trust, always verify, continuous authentication and authorization, and least privilege access (Rose et al., 2020). Each of these principles ensures that there is no implicit trust of any user or device, allowing for a safer environment. The parallel to Jeremiah 17:9 is clear here; just as the heart cannot be trusted by default, neither can users, devices, or network locations.

Penetration testing supports Zero Trust assumptions by actively testing whether controls actually enforce policy and that authentication and authorization behave as expected when under attack, making sure those controls actually work, and finally, uncovering implicit trust relationships (Rose et al., 2020; Scarfone et al., 2008). The principles of Zero Trust are evaluated using penetration testing in any given system, because, as we know, we can't even

trust that a system that says it is under Zero Trust actually is. Overall, Zero Trust Architecture shows us how to actually implement the biblical insight into a practical security model.

Conclusion

As we have seen throughout this essay, Jeremiah 17:9 offers a surprisingly accurate framework for understanding modern cybersecurity realities. The verse parallels false trust in networks, the need for testing to reveal hidden truths, human factors in security failures, and ethical restraint and humility in positions of power. Network penetration testing is not just a technical necessity, but it is an ethical service that is grounded in humility, realism, and responsibility. After this process, it has been further proven to me that integrating biblical insight with technical knowledge and skills strengthens both security and professional integrity.

Works Cited

Rose, S. , Borchert, O. , Mitchell, S. and Connelly, S. (2020), Zero Trust Architecture, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-207, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment (NIST Special Publication 800-115). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-115.pdf

Verizon Business. (2024). 2024 Data Breach Investigations Report: Executive summary (Verizon DBIR). Verizon Business. https://www.verizon.com/business/resources/reports/2024-dbir-executive-summary.pdf