Cyber Range Lab Assignment 4

Blockchain in Action

Jon Mahoney

SRA 440W

# General Context

Blockchain technology can be described as an electronic ledger that tracks a variety of things using digital signatures and consensus algorithms. Blockchain technology makes use of peer-to-peer network structures as well as multiple layers of systems and devices. In the “Blockchain in Action” course, the instructor describes different aspects of blockchain in four sections. These sections are “Process of Block Creation”, “Attacking Block Creation”, “Targeting the Node”, and “Attacking the Network”.

Process of Block Creation

In the introductory section, the speaker describes the basic processes of blockchain. For blockchain systems to be successful, they must transmit available transactions, come to a consensus on block creators and solvers, as well as building and validating the blocks. The incentive for people to participate in the blockchain process is monetary gain from validating the digital signature for blocks. In other words, people are working together to ensure the validity of payments in a public digital ledger. However, the process is not infallible which leads to exploitation of blockchain.

Attacking Block Creation

The next section describes the different ways the block creation process can be exploited. Due to the nature of a peer-to-peer blockchain network, denial of service attacks are often ineffective because there is no single point of necessity in the process. That being said, there are nodes that are more important than others and there are often bottlenecks which can be targeted for denial of service. Another way the block creation process can be exploited is through a method of artificially inflating the transaction values for solving and validating blocks called frontrunning. Frontrunning occurs when a node on the blockchain network notices a transaction broadcast and sends in its own transaction before finalization of the original transaction. Another exploitation of the block creation process is selfish mining where an individual may keep a block secret so they can solve a greater portion and earn more money in doing so. Ideally, people broadcast their blocks so the blocks can be solved as quickly as possible, but that allows for competition among miners.

Targeting the Node

The following section describes different ways individual nodes on the blockchain network can be attacked. Devices on the blockchain network can be exploited through their software configurations as well as being generally susceptible to malware. There is a known vulnerability in Etherium mining networks that certain processes will unintentionally open port 8445. This is problematic due to the fact that port 8445 is used to transmit information to crypto wallets and attackers can actually steal currency from crypto wallets by exploiting this misconfiguration. This also ties into our last lab assignment where we scanned a network of devices for open ports for the purpose of identifying vulnerabilities in a network.

# Attacking the Network

The final section addresses the way attackers can exploit communication between nodes on a blockchain network. Due to the nature of a peer-to-peer network, each node relies on the information provided by other nodes. Attackers can exploit this communication chain between nodes to influence blockchain consensus algorithms. Some noteworthy network attacks include Eclipse attacks, Routing attacks, and Sybil attacks. Eclipse attacks only separate a single node from the network while a routing attack will actually split the entire network into segments. Sybil attacks are incapable of altering blockchain consensus algorithms because they simply involve flooding a blockchain with malicious accounts.

# Certificate

