Protection Against Brute-force Attacks

Timothy Dao, Dillion Barnhardt
Advisor: Jose Gomez

Department of Integrated Information Technology
University of South Carolina
Agenda

• Description of Brute Force Attacks
• Objectives
• Scenario
• Mitigation
• Advantages of NGFW
• Conclusion
Description of Brute force Attacks

• Attacker sends packets using a variety of protocols to continuously attack a destination IP address with the motivation of discovering credentials.

• The attacker can gain access to classified information and critical systems.

Figure 1. Network topology.
Objectives

• Determine the effectiveness of a Next Generation Firewall (NGFW) in detecting brute-force attacks, while providing best practices when deploying a NGFW

• Implement a brute-force detection policy to detect and block malicious attacks using the SSH, FTP, Telnet, and HTTP protocols

• Use an open-source tool to such as Ncrack and Hydra to perform Brute force

• Prevent tools such as Ncrack and Hydra from discovering credentials on the network
Scenario

- Attack will use PC2 to attack PC1 using SSH, Telnet, FTP, and HTTP
- NGFWs uses signatures to protect PC1 from a brute force attack
Mitigation

• Vulnerability protection policy is enacted when traffic that matches the selected signatures is detected

• Policy is triggered once there is over a certain criteria of detected SSH, Telnet, FTP, and HTTP packets sent.

![Image of Vulnerability Protection Profile]
Advantages of NGFW

• Inspects incoming packets in depth to look for attack signatures and detect threats
• Features malware and Denial of Service (DoS) protection that detects and blocks malicious traffic from entering and affecting users on the network
• NGFWs can monitor traffic from layer 2 through 7, this allows for application and user-based policies
Conclusion

• NGFWs are effective in detecting and blocking Brute-force attacks

• Open-source tools that are available to the public can be utilized to perform a multitude of attacks on different protocols

• Keeping a record of logs and utilizing attack signatures are an effective way to detect and block attacks