Incident Postmortem: Firewall Bypass Incident

## **Summary**

In the late hours of March 20, 2022, at 03:21 UTC, a security incident happened where multiple unauthorize bypass action were logged in the firewall. The attack originated from an Australian IP address and targeted **nbn.external.network.** The attacker used POST requests on **/tomcatwar.jsp** with malicious payloads intended to exploit vulnerability in Telstra System. The incident raise concerns over firewall rule enforcement and web application security.

## **Impact**

* Potential **unauthorized access** to the **nbn.external.network**.
* Possible **web shell deployment** through **tomcatwar.jsp**, allowing remote execution.
* Firewall **failed to block** malicious requests, indicating misconfigurations or rule weaknesses.
* Increased **risk of data exfiltration or system compromise**.

## **Detection**

* The attack was discovered through **firewall logs**, which recorded **bypass actions** for multiple malicious IP addresses.
* The security team noticed unusual POST requests targeting /tomcatwar.jsp with suspicious payloads.
* No automated alerts were triggered, suggesting a need for improved monitoring.

## **Root Cause**

* **Weak firewall rules**: The firewall allowed bypass actions instead of blocking known attack patterns.
* **Insufficient WAF (Web Application Firewall) protections**: The malicious payloads were not properly filtered.
* **Lack of logging and alerting mechanisms**: No real-time notification of suspicious activity.
* **Possible unpatched vulnerability in the application** that allowed execution of unauthorized scripts.

## **Resolution**

* **Immediate firewall rule updates** to block the attacking IPs and tighten security around /tomcatwar.jsp.
* **Web Application Firewall (WAF) enhancement** to detect and block malicious payloads.
* **System integrity check** to ensure no unauthorized access was achieved.
* **Security patching** of any identified vulnerabilities in the application.

## **Action Items**

1. **Review and refine firewall rules** to prevent future bypass actions.
2. **Deploy enhanced WAF rules** to detect and block attacks targeting web applications
3. **Implement automated alerting** for suspicious activities in firewall logs.
4. **Conduct penetration testing** to identify other security gaps.
5. **Patch vulnerable** applications and enforce secure coding practices.
6. **Regularly review and update security misconfigurations and configurations** in response to evolving threats.