20 Security Tools used In DevOps By DevOps Shack

1. **SonarQube (SAST):**
    - **Description:** SonarQube is a static code analysis tool that helps identify code quality issues, bugs, and security vulnerabilities.
    - **Example:** SonarQube
2. **OWASP ZAP (DAST):**
    - **Description:** ZAP is an open-source dynamic application security testing tool used for finding vulnerabilities in web applications during runtime.
    - **Example:** OWASP ZAP
3. **Contrast Security (IAST):**
    - **Description:** Contrast Security provides interactive application security testing, offering continuous monitoring and protection for applications.
    - **Example:** Contrast Security
4. **Anchore (Container Security):**
    - **Description:** Anchore scans container images for vulnerabilities, policy violations, and provides insights into container security.
    - **Example:** Anchore
5. **HashiCorp Vault (Secrets Management):**
    - **Description:** Vault manages secrets and protects sensitive data, providing centralized secret management and secure access.
    - **Example:** HashiCorp Vault

6. **Checkov (IaC Security):**
    - **Description:** Checkov is an IaC security tool that scans infrastructure-as-code files for security misconfigurations.
    - **Example:** Checkov
7. **Prometheus and Grafana (Continuous Monitoring):**
    - **Description:** Prometheus is a monitoring and alerting toolkit, and Grafana is used for visualization. Together, they provide powerful monitoring capabilities.
    - **Examples:** Prometheus, Grafana
8. **ELK Stack (SIEM):**
    - **Description:** ELK Stack combines Elasticsearch, Logstash, and Kibana for log management and analysis, helping in identifying security incidents.
    - **Examples:** Elasticsearch, Logstash, Kibana
9. **Nessus (Vulnerability Scanning):**
    - **Description:** Nessus is a widely-used vulnerability scanner that identifies and helps remediate vulnerabilities in systems and applications.
    - **Example:** Tenable Nessus
10. **Demisto (SOAR):**
    - **Description:** Demisto (now part of Palo Alto Networks Cortex XSOAR) is a Security Orchestration, Automation, and Response platform for incident response automation.
    - **Example:** Cortex XSOAR
11. **Snort (Intrusion Detection and Prevention System):**
    - **Description:** Snort is an open-source IDS/IPS that monitors network traffic for malicious activity and helps prevent security breaches.
    - **Example:** Snort
12. **Clair (Container Image Security):**
    - **Description:** Clair is an open-source project for the static analysis of vulnerabilities in application containers.
    - **Example:** Clair

13. **Sysdig Secure (Container Security):**
    - **Description:** Sysdig Secure provides container security and monitoring, offering runtime protection and visibility.
    - **Example:** Sysdig Secure
14. **Aqua Security (Container Security):**
    - **Description:** Aqua Security specializes in container security, providing comprehensive solutions for securing containerized applications.
    - **Example:** Aqua Security
15. **Arachni (Web Application Security Scanner):**
    - **Description:** Arachni is an open-source web application security scanner designed to find security issues in web applications.
    - **Example:** Arachni
16. **OpenVAS (Open Vulnerability Assessment System):**
    - **Description:** OpenVAS is an open-source vulnerability scanner used to perform comprehensive vulnerability assessments.
    - **Example:** OpenVAS
17. **GitSecrets (Git Repository Scanning):**
    - **Description:** GitSecrets scans Git repositories for sensitive information like passwords and API keys, helping prevent accidental leaks.
    - **Example:** GitSecrets
18. **Trivy (Container Image Security):**
    - **Description:** Trivy is a simple and comprehensive vulnerability scanner for container images, focusing on simplicity and speed.
    - **Example:** Trivy
19. **Wazuh (Host-based Intrusion Detection System):**
    - **Description:** Wazuh is a security information and event management (SIEM) tool with host-based intrusion detection capabilities.
    - **Example:** Wazuh

20. **GitLab CI/CD (Integrated Security):**
    - **Description:** GitLab CI/CD, when configured with security scanners and tools, provides integrated security checks within the development pipeline.
    - **Example:** GitLab CI/CD

These tools collectively address various aspects of security within a DevOps environment, covering code analysis, container security, infrastructure security, incident response, and more. The specific choice of tools depends on the organization's needs, infrastructure, and security requirements. Integrating multiple tools into the DevOps pipeline helps create a robust security posture.