PD
PENTEST DIARIES

PD
PENTEST DIARIES
HTTPS://WWW.SAKSHAMDIXIT.COM

KNOWLEDGE SHARE

PENTEST DIARIES

@pentestdiaries

1000+ IP addresses tried to hack our new Ubuntu box in the last 8 days

That many attempted intrusions in such a short period on a new Ubuntu box definitely warrants attention. Here's how to approach the situation:

Immediate Steps:

1. **Change SSH Password:** **If you haven't already, immediately change the default SSH password on your Ubuntu box. Use a strong, unique password and consider using SSH key authentication for added security. Here's a guide for beginners: https://superuser.com/questions/404701/how-to-reset-default-ssh-password-in-ubuntu**
2. **Review Firewall Rules:** **Make sure your firewall is enabled and configured to only allow access to authorized services (like SSH) on specific ports. You can use tools like UFW (Uncomplicated Firewall) to manage firewall rules easily: https://help.ubuntu.com/community/UFW**
3. **Secure Other Services:** **If you're running other services on your Ubuntu box (web server, database), ensure they are properly configured and patched to address any known vulnerabilities.**
4. **Update and Patch:** **Ensure your Ubuntu system is up-to-date with the latest security patches and updates. Vulnerabilities in outdated software versions can be exploited by attackers.**

Investigate Further:

1. **Log Analysis:** **Check your system logs (especially SSH logs) to see details about the attempted intrusions. This might give you clues about the source of the attacks and the methods used. You can use tools like `logwatch` to analyze logs.**
2. **Identify Vulnerabilities:** **Use a vulnerability scanner like OpenVAS to identify potential weaknesses in your system configuration or software. This can help you prioritize patching any critical vulnerabilities. https://www.openvas.org/**

Additional Security Measures:

- **Disable Root Login:** Consider disabling root login via SSH and use a standard user account with sudo privileges for administrative tasks.
- **Two-Factor Authentication (2FA):** Implement 2FA for SSH or other services to add an extra layer of security.
- **Keep Software Updated:** Make sure your Ubuntu system and all installed software are up-to-date with the latest security patches.

Strengthen Security Measures:

- **SSH Configuration:** If SSH is accessible, secure it by:
  - Disabling root login and using a non-standard port if feasible.
  - Enforcing strong passwords or better yet, using SSH keys for authentication.
- **Access Control:** Limit access to services and applications based on the principle of least privilege. Review user accounts and permissions regularly.

Intrusion Detection and Prevention:

- **Intrusion Detection Systems (IDS):** Consider installing and configuring IDS software like `Snort` or `Suricata` to detect and respond to suspicious activities in real-time.
- **Honeypots:** Deploy honeypot systems to lure attackers away from critical infrastructure and gather information about their methods and origins.

Seeking Help:

- **Online Resources:** The Ubuntu community forums and security resources provide valuable information and troubleshooting steps. https://help.ubuntu.com/
- **Security Professional:** If you're not comfortable handling these tasks yourself, consider seeking help from a security professional to assess your system and implement necessary security measures.

Reporting and Collaboration:

- **Security Team or Provider:** **If applicable, notify your organization's security team or service provider to coordinate efforts and potentially block IP addresses at a network level.**

Continuous Monitoring and Learning:

- **Learn from Incidents:** **After addressing the immediate threats, conduct a thorough post-incident analysis to identify vulnerabilities and weaknesses in your security posture.**
- **Educate Users:** **Raise awareness among users about cybersecurity best practices, such as recognizing phishing attempts and using strong, unique passwords.**

Mitigating Future Attacks:

By taking these steps, you can significantly harden your Ubuntu box's security posture and reduce the risk of successful attacks in the future. Remember, security is an ongoing process, so stay vigilant and keep your system updated.

Additional Considerations:

- **Network Segmentation:** **Consider segmenting your network to isolate critical systems and reduce the impact of potential breaches.**
- **Penetration Testing:** **Periodically conduct penetration testing to proactively identify and address vulnerabilities before attackers exploit them.**

Response Plan:

- **Incident Response Plan:** **Develop or review an incident response plan that outlines steps to detect, respond to, and recover from security incidents effectively.**
- **Backup:** **Ensure critical data is regularly backed up and stored securely to facilitate recovery in case of a successful breach or data loss.**