

Incident Response

- ❖ *DigitalSherlock.com | SafeHack.com*
- ❖ *Date: 2005/05/27*
- ❖ *Document Name: incident_response*
- ❖ *GNU Free Documentation License*
- ❖ *Version 1.00, 2005-05-27*
- ❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*
- ❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

❖ Help To

- **Find out what happened**
- **Find How it happened**
- **Find Who did it**
- **Find Why they choose your Network**
- **Create a record of the incident**
- **Create a record to observe trends**
- **Create a record to improve processes**
- **Avoid confusion**

❖ Accepted Steps

- **Preparation**
 - **limits the potential for damage**
- **Identification**
 - **Identification is a difficult process**
 - **There are many false positives**
 - **Can be identified by users**
 - **Can be identified by system support**
 - **IDS system / Firewall**
 - **Classifications**
 - **Unauthorized Privileged**
 - **Unauthorized Limited (user) Access**
 - **Unauthorized Unsuccessful Attempted Access**
 - **Unauthorized Probe**
 - **Poor Security Practices**
 - **Denial of Service (DOS) Attacks**
 - **Malicious Logic**
 - **Hardware/Software Failure**
 - **Unauthorized Utilization of Services**
- **Containment**
 - **limiting the magnitude of an incident**
 - **We should start containment As soon as detected**
- **Eradication**
 - **removing the cause of the incident**
- **Recovery**
 - **restoring the system**
- **Follow-up**

- **Is a Critical Process**
- **improve incident handling**
- **Address efforts to prosecute**
- **Analyze the Incident and the Response**
- **Analyze the Cost of the Incident**
- **Prepare a Report**
- **Revise Policies and Procedures**
- **Lesson Learned**