NORMA TÉCNICA PARA IMPLEMENTAÇÃO DE MECANISMOS DE SEGURANÇA EM SISTEMAS UNIX

Referência: NT-AI.01.05.01

http://intranet.unesp.br/ai/regulamentos/nt-ai.01.05.01.pdf

Data: 16/09/1998

STATUS: EM VIGOR

A Assessoria de Informática, órgão executivo responsável pela normatização e padronização de procedimentos referentes à área de informática, de acordo com o Regulamento Geral para Uso e Administração de Computadores e Redes da Unesp (RG-AI.00.01.01, Portaria UNESP 65/98), define a seguinte NORMA TÉCNICA:

1. RESUMO

Este documento estabelece normas e procedimentos para implementação de mecanismos de segurança em sistemas UNIX, sendo complementar ao Regulamento Geral para Uso e Administração de Computadores e Redes da Unesp (http://intranet.unesp.br/ai/regulamentos/reg_geral.htm).

2. PALAVRAS CHAVES

Segurança, Redes de Computadores, Internet, TCP/IP, TCPWrapper, Cracker, Tripwire, Senhas, unespNET

3. NORMA TÉCNICA

Os itens aqui descritos fazem parte dos procedimentos padrão de segurança de servidores UNIX. Caso hajam dúvidas com relação à implementação deve-se recorrer ao Grupo de Redes de Computadores (GRC) da Unesp, através do *e-mail*: suporte-redes@unesp.br.

Devem ser adotados os seguintes procedimentos de segurança em servidores e estações de trabalho conectados à unespNET:

3.1 Contas de Acesso ao Sistema

3.1.1 Cada usuário deve possuir uma conta individual. Não devem haver contas corporativas, ou cuja senha seja compartilhada por mais de uma pessoa, exceto em situações especiais e por prazos curtos e pré-determinados. Vide item 3.7.1 do Regulamento Geral.

3.1.2 Cada conta deve possuir uma senha, sendo que esta deve seguir as seguintes regras de formação:

- Deve possuir no mínimo 8 caracteres;

- Deve possuir no mínimo dois caracteres que não sejam parte do alfabeto;
- Não devem ser utilizadas palavras encontradas em dicionários (de língua portuguesa ou estrangeira);
- Não devem ser utilizadas palavras invertidas.

3.1.3 Deve ser executado periodicamente o programa *Cracker* versão 5.0, que tenta quebrar senhas frágeis. O usuário que possuir sua senha quebrada deve ter seu acesso bloqueado por, no mínimo, uma semana e passar por um processo de conscientização a respeito do uso de senhas fortes. O acesso só pode ser restabelecido após o processo de conscientização. A cada reincidência acrescenta-se uma semana ao prazo de bloqueio anterior, chegando-se a, no máximo, 6 meses de bloqueio.

3.1.4 Ao usuário root deve ser permitido *login* somente no console da máquina.

3.1.5 Deve ser atribuído o *shell* /bin/false às contas: daemon, bin, sys, adm, uucp, nobody, lpd, netinst e ftp. Vide Regulamento Geral item 3.6.

3.1.6 As contas guest e similares devem ser removidas do sistema. Vide Regulamento Geral item 3.7.1.

3.2 Serviços

3.2.1 Devem ser desabilitados os serviços: rlogin, rexec, rsh, rquota, rex, rstat, rusers e rwall. Caso haja justificativa e extrema necessidade de uso destes serviços, o administrador deve:

i. Certificar-se de que não existe nenhum arquivo .rhosts com conteúdo que possibilite *login* remoto sem senha em uma conta do sistema.
ii. Certificar-se da inexistência de falhas de segurança nos processos servidores a serem utilizados.
iii. Manter análise e auditoria rigorosa do acesso a esse serviço, em conjunção a aplicação de proteção e *logging* por intermédio do *TCPWrapper* (vide item 3.3.3 desta norma).

3.2.2 Deve ser desabilitado o serviço tftp, exceto em casos de extrema necessidade de utilização do mesmo.

3.2.3 Deve ser desabilitado o serviço de NFS em máquinas que não sejam servidoras de arquivos. Nas máquinas em que o serviço de NFS estiver habilitado, deve-se cuidar para que os sistemas de arquivos sejam exportados somente para as máquinas que necessitam acessá-los e com permissão de escrita somente quando necessário.

3.3 Aplicativos e Métodos

3.3.1 Todas as máquinas servidoras devem manter em execução o *daemon* syslog para possibilitar o controle dos *logs* de eventos do sistema. Vide Regulamento Geral item 4.4.

3.3.2 Deve ser utilizado o *software Tripwire* versão 1.2, para gerar uma base de dados certificada do sistema. Vide Regulamento Geral itens 3.5 e 5.3.

3.3.3 Deve ser instalado o *software TCPWrapper* versão 7.6 em todas as máquinas servidoras. Este deve ser configurado de forma a impedir o acesso, aos serviços por ele controlados,

a partir de máquinas que não estejam explicitamente autorizadas pelo administrador da rede. Vide Regulamento Geral itens 3.8 e 5.3.

3.4 De acordo com o Item 5.3 do Regulamento Geral, obrigatoriamente, devem ser seguidos todos os procedimentos descritos nos Alertas de Segurança, distribuídos eletronicamente pelo Grupo de Redes de Computadores da Assessoria de Informática, através da lista de discussão SYSMAN-L@UNESP.BR.

3.5 Aplicação de procedimentos e eventos de segurança têm **prioridade máxima** com relação às demais atribuições e serviços de administração de rede.

3.6 Incidentes de segurança

3.6.1 Devem ser coletados todos os logs disponíveis a respeito do incidente de segurança e enviados via *e-mail* para CERT-UNESP@UNESP.BR. Se possível, estes *e-mails* devem ser criptografados com PGP.

3.6.2 Deve ser preenchido o **Formulário Para Informação de Incidente** do GRC - Unesp (vide Anexo I). Podendo este formulário ser enviado via *e-mail* para CERT-UNESP@UNESP.BR ou preenchido diretamente em http://grc.unesp.br/formularios/incidente.html.

3.6.3 Considerando os seguintes incidentes específicos ou similares:

- Onde alguém tenha conseguido acesso ilícito a alguma conta do sistema, ou
- Onde alguém tenha conseguido acesso à conta de root do sistema, ou
- Onde possa ter havido a execução remota de algum código com permissão de root;

então a máquina deve ser considerada como possivelmente comprometida. Neste caso a mesma deve ser retirada imediatamente da rede e adotadas as providências definidas nos itens 3.6.1 e 3.6.2, acima.

Anexo I

GRC - Unesp
Formulário para Informação de Incidente

Versão 1.0
Data: 16/Set/1998

O Grupo de Redes de Computadores da Unesp desenvolveu o seguinte formulário no intuito de padronizar a notificação de incidentes relativos à segurança. Por favor preencha o formulário da forma mais detalhada possível, isso facilitará enormemente o auxílio prestado, embora não seja necessário preenchê-lo completamente.

É importante lembrar que as informações relativas ao seu site serão tratadas de forma confidencial.

Por favor retorne este para cert-unesp@unesp.br

Grato por sua cooperação e ajuda.

_____

1. Informações gerais

1.1. Incidente Número (Preenchimento reservado ao GRC): GRC#

1.2. Sobre o Site

1.2.1. Nome do site:
1.2.2. Nome do Domínio:

2. Contato Técnico

2.1. Nome:
2.2. E-mail:
2.3. Telefone:
2.4. FAX:
2.5. Canal de comunicação seguro (preferencialmente PGP) (Sim/Não):

2.5.1 Se sim, qual?:

2.6. Contatos adicionais (Se disponível)

2.6.1. Nome:
2.6.2. E-mail:
2.6.3. Telefone:
2.6.4. FAX:
2.6.5. Canal de comunicação seguro (preferencialmente PGP) (Sim/Não):

2.6.5.1 Se sim, qual?:

3. Informações descobertas

3.1. Por favor informe todas as suas máquinas envolvidas no incidente

3.1.1. Nome(s) do(s) Host(s):
3.1.2. Endereço(s) IP:
3.1.3. Hardware, S.O., e versão:
3.1.4. Existem Patches de segurança aplicados/recomendados pelo fabricante e boletins de segurança? (Sim/Não/Desconheço):

3.1.5. Função(ões) do(s) host(s) informado(s)

3.1.5.1. Roteador (Sim/Não):
3.1.5.2. Servidor de Comunicação (Sim/Não):
3.1.5.3. Outro:

3.1.6. Este equipamento ficou comprometido após o ataque? (Sim/Não):

3.2. Host(s) de outros(s) sites envolvidos no ataque

3.2.1. Nome(s) do(s) Host(s):
3.2.2. Endereço(s) IP:
3.2.3. Hardware, S.O. e versão:
3.2.4. neste ataque, este(s) hosts são atacante(s), vítima(s), ou ambos?:

4. Categorias de incidente (Por favor marque todas as categorias relevantes)

4.1. Rastreamento de portas(s):
4.2. Email Falsificado:
4.3. Email bomb:
4.4. Spam:
4.5. Telefonia:
4.6. Engenharia social:

4.7. Ataque baseado em Sendmail:

4.7.1. Este ataque comprometeu a segurança do servidor?
(Sim/Não/Não posso afirmar)

4.8. Invasão

4.8.1. Intruso obteve acesso privilegiado (root)?
(Sim/Não/Não posso afirmar)

4.8.2. Intruso instalou algum cavalo de troia(s)?
(Sim/Não/Não posso afirmar)

4.8.3. Intruso instalou algum sniffer (Sim/Não/Desconheço):

4.8.3.1. Informações sobre o log do sniffer:

4.8.4. Ataque a NIS:
4.8.5. Ataque a NFS:
4.8.6. Ataque a TFTP:
4.8.7. Ataque a FTP:
4.8.8. Ataque a Telnet:
4.8.9. Rlogin ou rsh:
4.8.10. Quebra de senhas:
4.8.11. Acesso através de usuário sem senha:

4.9. Utilização impropria do FTP:
4.10. IP spoofing:
4.11. Produto vulnerável (qual):
4.12. Erro de configuração (qual):

4.13. Algum destes ataques retirou algum serviço ou o servidor do ar? (Sim/Não):

5. Ferramentas de segurança

5.1. Descreva a(s) existentes no(s) host(s) vítima(s):

5.2. Descreva os logs possíveis de recuperar após a invasão:

6. Descrição detalhada do incidente:

6.1. Data e duração do incidente:
6.2. Como você descobriu o incidente:
6.3. Método usado para ganhar acesso ao(s) host(s):
6.4. Arquivos/diretórios escondidos:
6.5. Fonte do ataque (se conhecida):
6.6. Atitudes tomadas até o momento em relação ao(s) host(s) afetados:

6.7. Saída do programa do(s) pacotes usados na invasão:

6.8. Ferramentas e programas usados para explorar a(s) vulnerabilidade(s):

6.9. Código fonte do(s) programa(s) usados na invasão:

6.10. Binário do(s) programa(s) usado(s) na invasão
(recomendamos fortemente enviar em e-mails em separado, criptografados com PGP):

6.11. outros arquivos relevantes:

Este documento foi escrito baseado no "Formulário para informação de incidente" do CERT-BR.

Fim de documento - 16/09/1998
Este documento pode ser obtido em
http://intranet.unesp.br/ai/regulamentos/nt-ai.01.05.01.pdf