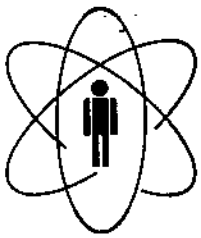
ISSN 0101-9201



CBPF - CENTRO BRASILEIRO DE PESQUISAS FÍSICAS
Rio de Janeiro

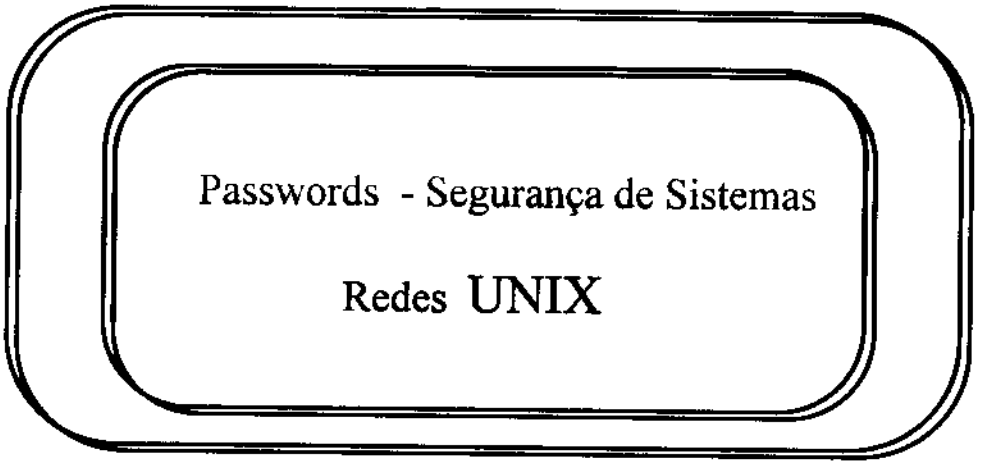
Notas Técnicas

CBPF-NT-002/94
November 1994

Passwords – Segurança de Sistemas Redes UNIX

Marita Maestrelli & Mário Henrique de Sá Vera

CNPq - Conselho Nacional de Desenvolvimento Científico e Tecnológico



Marita Maestrelli
Mário Henrique de Sá Vera

Centro Brasileiro de Pesquisas Físicas - CBPF

C A T - Informática

Rua Dr. Xavier Sigaud , 150

22290 - 180 - Rio de Janeiro / RJ , Brasil

Objetivo

Com o rápido crescimento das Redes Nacionais e Internacionais de Computadores , a questão da Segurança em Sistemas tornou-se de grande importância.

O que antes era tema de filmes de Ficção sobre "hackers" (intrusos e outros) , com o aparecimento dos Processadores de alta velocidade virou uma perigosa realidade . Este estudo evidencia a fragilidade com que se encontra a maioria das Redes de usuários. Várias técnicas usadas pelos "hackers" foram colocadas explicitamente (o que é discutível em termos de quem está tendo acesso a estas informações !) , e finalmente, este documento propõe o desenvolvimento de um aplicativo (**"Checker"**) , que fará parte do Projeto que visa o aumento da segurança da Rede UNIX do Centro Brasileiro de Pesquisas Físicas.

Índice

Segurança nos Sistemas de Redes Unix

Introdução

A Segurança das contas e Passwords sempre foi assunto rotineiro entre Profissionais e usuários de Unix . Nos primórdios do Unix,o algorítmo de Criptografia era uma simulação do usado pelo M-209, máquina (cipher) usada na segunda Guerra Mundial . Na época,este algorítmo era eficaz e bem rápido,apesar de suas fraquezas . Exemplificando,num PDP-11/70 cada Criptografia levava cerca de 1.25 ms. Desta forma,podia-se comparar cerca de 800 Passwords/segundo . Acessando um Arquivo Dicionário com 250.000 palavras um *"hacker"* poderia testar suas palavras Criptografadas,com todas contidas no arquivo de Password de um Sistema qualquer ,em pouco mais de 5 minutos . Isto era um furo na segurança dos Sistemas da época .

Nas últimas versões do Unix,um novo algorítmo foi usado para criptografar as Passwords - DES (Data Encryption Standard) . Com este novo algorítmo um *"hacker"* teria um gasto de cerca de 40 dias de CPU para testar todas as palavras Criptografadas com as de um Sistema de 50 contas (isso usando um VAX-II que é bem mais veloz do que o PDP-11/70). Este novo algorítmo era mais lento do que seu antecessor,e também construia as Passwords com 11 caracteres,mais 2 de "salto" aleatório . Desta forma,achou-se que o problema estava resolvido .

Porém,alguns novos fatores foram introduzidos,e trouxeram novamente à tona o problema de segurança de Sistemas :

1- Acesso de usuários comuns a Workstations com velocidade de CPU cerca de 25-40 vezes maior do que um PDP-11/70 . Literalmente,o poder computacional disponível aos *"hackers"* hoje é milhares de vezes maior do que há dez anos atrás .
2- Novas versões do algorítmo DES foram desenvolvidas tal que permitem a Criptografia do mesmo Arquivo Dicionário,seguida por uma comparação com as Passwords criptografadas,abaixo da barreira de 1ms . E para tornar a situação ainda mais preocupante, com o uso da Computação Paralela este mesmo Dicionário de 250.000 palavras pode ser rastreado e ter muitas de suas Passwords reconhecidas em apenas alguns segundos .
3- Cada vez mais os Sistemas tendem a fornecer ambientes Multi-Usuários.Porém,a grande maioria dos usuários subestimam,ou desconhecem, o poder de um *"hacker"* malicioso,que ao entrar em suas contas pode causar danos não apenas à esta determinada conta,em específico,como a maioria pensa,mas infelizmente danificar todo o Sistema .

Uma abordagem de muitos Administradores de Redes Unix,tem sido o de rastrear o próprio arquivo de Passwords de sua Rede,e avisar os usuários que ele conseguiu "reconhecer" (igualar) a Criptografia da Password . Isso ainda não é de todo suficiente porque não garante que um "*hacker*" provido de um Arquivo Dicionário mais completo consiga reconhecer Passwords que o Administrador não conseguiu .

Uma solução que vem sendo bastante adotada é a de tornar o arquivo '/etc/passwd' ilegível,ou fazer uma divisão deste em duas partes - um arquivo '/etc/passwd' legível com tudo presente menos a parte das Passwords criptografadas,e uma parte "shadow" que seria legível apenas ao '*ROOT*' (proposta pela Sun Microsystems) .

A solução proposta aqui é de se ter na Rede, um Rastreador de Passwords que seja acionado toda vez que o usuário modificar ou criar a Password . Um segundo passo seria insistir na conscientização da questão de Segurança,por parte dos usuários (o que já seria um grande progresso) . Estes Rastreadores estão disponíveis em domínio público,os Administradores interessados (para ter acesso a Rastreadores poderosos deve-se seguir certas exigências) devem consultar a Bibliografia.

Desenvolvimento

1) Vulnerabilidade de uma Rede :

Já é há muito sabido que tudo que um *"hacker"* precisa fazer para ter acesso a uma máquina Unix é seguir dois simples passos :

1- Adquirir uma cópia do arquivo '/etc/passwd' atraves de algum tipo de Protocolo de Comunicação . (ftp,uucp, etc...)
2- Aplicar uma versão do algorítmo de Criptografia sobre uma série de palavras,tipicamente '/usr/dict/words',juntamente com permutações com o nome do usuário, e finalmente comparar os resultados sobre os achados no arquivo '/etc/passwd' .

Caso uma tentativa seja satisfeita (e geralmente se obtem sucesso em pelo menos uma !),então o *"hacker"* tem acesso a máquina alvo . A maioria dos usuários já conhece este método de ataque,porém poucos preocupam-se em se defender. Muitos usuários colocam ,inclusive,combinações com as palavras de seu próprio nome para servir de Password . Este tipo de Password um *"hacker"*,iniciante,consegue reconhecer em menos de um segundo .

O que resta aos Administradores de Redes é desenvolver métodos que evitem o emprego de Passwords fracas,já que a comodidade de certos usuários (desinformados na maioria das vezes sobre o perigo de se ter uma Password nula,por exemplo !) pode causar sérios problemas para todos nós . E ainda insistir num tema de grande importância para todos usuários,e que vem se tornando assunto prioritário a nível mundial : "Usuários bem educados e informados é sinônimo de Rede segura !"

Para os usuários que desconhecem os danos que um intruso mal intensionado pode causar à uma Rede ,vamos listar alguns simples exemplos :

+ Execução de Processos pesados nas máquinas principais,causando lentidão do Sistema.

+ Remoção de todos os arquivos de usuários, que porventura tenham permissão global ("world") .

2) Analisando Passwords :

Para manter uma Rede em razoável segurança,é preciso em primeiro lugar,haver uma conscientização de seus usuários sobre o assunto . Em segundo lugar ,um policiamento periódico sob as Passwords que estão sendo criadas e substituídas pelos usuários . Este segundo item é justamente o tópico central deste trabalho : - como fazer a manutenção de uma Rede de um número razoável de usuários,sem precisar fazer do Supervisor uma "babá" dos que usam Passwords pífias,e às vezes até nulas ?

Uma boa Password é aquela que é fácil de ser lembrada e difícil de ser quebrada . O problema é que na decisão entre uma Password de fácil memorização,e uma segura,o usuário quase sempre opta pela primeira opção . As Passwords aleatórias são as melhores em termos de segurança,ainda mais se forem usados caracteres randômicos ("T+h@Z-*&"),porém estas são extremamente difíceis de serem memorizadas . O mesmo ocorre com o uso de palavras sonoricamente fáceis de serem pronunciadas ("BlasQBlom") . Nestes casos o usuário acaba usando tais Passwords por um curto período de tempo e joga fora.Ou recorre ao velho,e inútil, hábito de anotar a Password em um papel. Então o que fazer ?

Os Profissionais responsáveis pela segurança de Sistemas de alto risco de penetração costumam desenvolver seus próprios algorítmos de Criptografia . Como não esperamos que usuário nenhum faça o mesmo,uma sugestão é a de memorizar uma frase qualquer que tenha a ver com o cotidiano do usuário . Por Exemplo :

" O CBPF fica na rua Xavier Sigaud 150 "

nos daria a Password - OCfnrXS1,formada pelos caracteres iniciais de cada palavra/número da frase .Só para exemplificar,esta Password se caracteriza por uma combinação aleatória (se analisada sem qualquer tipo de informação quanto ao método de criação),de letras maiúsculas e minúsculas,contendo ainda números . Seria uma tarefa bastante heróica,até mesmo para o "*hacker*" mais dedicado,reconhecer esta Password . Esta Password ,de fácil memorização ,levaria cerca de 5 anos de CPU, usando uma DECstation 3100 com 1000 comparações por segundo . Nada mal hein ? Neste exemplo,mesmo que conseguissem reconhecer a Password,nenhum usuário precavido mantém sua Password por 5 anos .

Num mundo ideal,existiriam somente Passwords com oito caracteres,e que não estivessem em nenhum Arquivo Dicionário,com no mínimo um caracter especial (pontuação,numeral ou simbólico .) misturado com as letras,que por sua vez seriam maiúsculas e minúsculas . Porém,este grau de segurança é utópico (principalmente

quando se trata de usuários) . Porém,é possível separar alguns tópicos envolvendo regras que devem ser evitadas na criação de uma Password :

- O uso de combinações com as palavras do próprio nome do usuário,já que o nome do usuário fica descrito no arquivo de Passwords juntamente com a Criptografia de sua Password. Desta forma este é o primeiro teste feito pelos *"hackers"* .
- Não se deve usar palavras contidas no arquivo de palavras do Sistema ('/usr/dict/words'), mesmo que alteradas por um caracter especial .
- Passwords em geral devem conter no mínimo 8 caracteres .
- Passwords que não contém nenhum tipo de mistura entre letras maiúsculas e minúsculas,números ou caracteres especiais são,com certeza,as mais fáceis de serem reconhecidas .

3) Testes Práticos :

Bem,para não ficarmos na teoria,vamos analisar algumas Estatísticas . Tendo adquirido,via ftp,o pacote para Rastreamento de Passwords : "Crack (by Alec D. E. Muffet)" *, a Coordenação de Atividades Técnicas do Centro Brasileiro de Pesquisas Físicas (CAT - CBPF),passou a fazer testes mensais sobre as Passwords dos usuários de sua própria Rede de WorkStations.

Foge ao intuito deste trabalho,explicar o funcionamento do Rastreador Crack. Isto porque além de não querer dar informações importantes à pessoas erradas,maiores informações sobre este programa encontram-se no documento referenciado na Bibliografia . Porém , resumindo rápidamente seu funcionamento,e da maioria dos Rastreadores, o Crack utiliza o algoritmo padrão - DES (Data Encryption Standard) - utilizado pelo Sistema Operacional UNIX V , para criptografar as palavras de entrada.Como a maioria dos Sistemas Operacionais fornece os nomes,na maioria das vezes completo, dos usuários da Rede no próprio arquivo de Passwords do Sistema ('/etc/passwd') ,o Crack usa este arquivo,como entrada, no primeiro passo de sua busca. Nesta fase,ele reconhecerá a maioria das Passwords formadas pela combinação das sílabas/palavras dos nomes dos usuários.O segundo passo consiste em criar um grande Arquivo Dicionário formado à partir de um conjunto de arquivos,que já vem com o Software,mais um acesso ao arquivo '/usr/dict/words' do Sistema, onde será feita a pesquisa.Dependendo da área de aplicação,outros Dicionários são fornecidos,de acordo com a característica mais gerais dos usuários de cada Rede.Por exemplo,nossa Rede é formada por Pesquisadores da área de Física,logo,um *"hacker"* incluiria,certamente,um arquivo contendo nomes desta área.

Fica bem claro aqui que,na verdade,o Administrador que fizer uso do Crack em sua Rede,estará sendo um *"hacker"* própriamente dito.Se uma pesquisa preventiva consegue reconhecer uma Password,é porque a situação é de risco.Já que a pesquisa dos *"hackers"* não é preventiva...

Em nossa pesquisa,fornecemos ao Crack o arquivo 'etc/passwd' da Rede Sun,mais alguns arquivos,contendo :

+ Nomes Comuns . (Principalmente Femininos)
+ Nomes de Lugares .
+ Termos específicos da área de Física .

e somados a estes,foram incluidos os arquivos que o próprio Crack carrega consigo,mencionados anteriormente.

Os resultados só vieram a confirmar a necessidade imediata de se aumentar a segurança de nossa Rede de WorkStations.

O quadro a seguir mostra os resultados obtidos pela pesquisa feita no mês de Novembro :

Tipo de Password	*Tamanho do Dicionário*	*Nº de Acertos*	*%*
Nome do usário	240	5	2.08%
Nomes Comuns	106	7	2.91%
Cidades/Bairros	56	0	0%
Termos Científicos	36	4	1.66%
'/usr/dict/words'	25144	6	2.50%
Password "default"	1	34	14.16%
bad_passwd/jargon	1415	9	3.75%
Total	26998	65	27.06%

Quanto ao número de caracteres usados,a Estatística foi de :

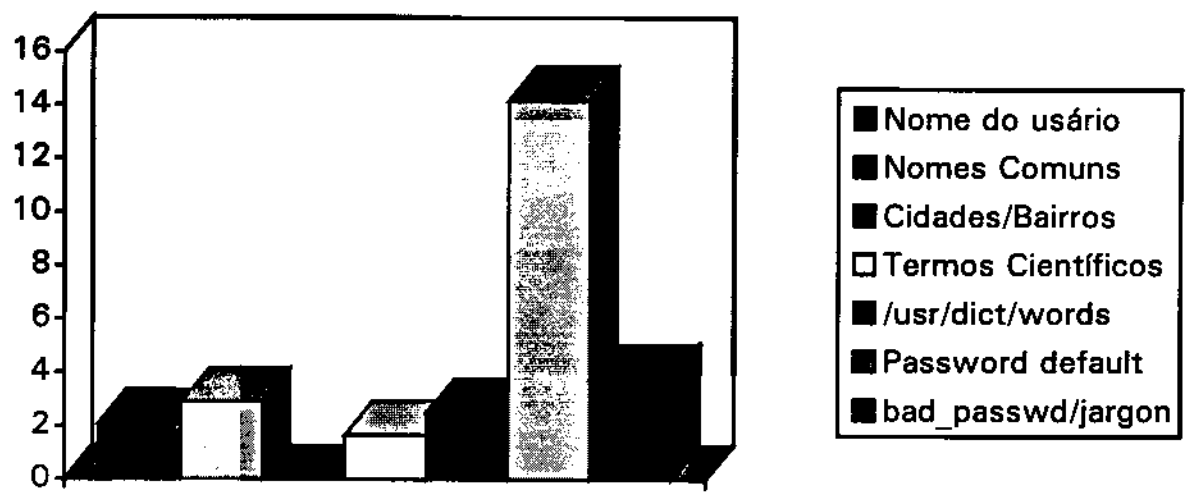
Nº de Caracteres	*Nº de Acertos*
5 Caracteres	1
6 Caracteres	19
7 Caracteres	8
8 Caracteres	5
Total	33

Obs. Não foi inserido na tabela com o número de Caracteres,a Password "default".

Devemos elucidar o fato de que ao analisarmos a Tabela com o número de caracteres mais frequêntes entre as Passwords reconhecidas,chega-se a conclusão de que uma Password com muitos caracteres não significa necessáriamente uma boa Password

(como certos usuários com nomes longos) .É perfeitamente possível criar-se Passwords bem protegidas com apenas seis caracteres.

Tipos de Passwords



Estes resultados,nos alerta para o fato de que os usuários não se interessam em mudar a Password "default" fornecida no momento de abertura de sua conta. Isto gera uma situação de alto risco,inclusive internamente,já que todos sabem a Password "default".

A simples presença de um Rastreador de Passwords na Rede já inibe os usuários mais despreocupados,ou devo dizer desinformados. Os resultados obtidos no primeiro mês (Outubro) foram catastróficos. Existia uma série de usuários sem Password alguma (NULA!).Desta forma,é somente digitar o nome do usuário e você está dentro do Sistema.Porém já no segundo mês não detectou-se mais a presença de Passwords nulas.

É bastante compreensível que muitos usuários usem os nomes de suas esposas,ou filhas, como Password.Tais senhas são bastante fáceis de serem lembradas.Porém,um dos Arquivos Dicionário do *"hacker"* menos dedicado,certamente conterá nomes femininos.Pode parecer difícil,mas criar uma Password bem protegida é mais fácil do que se imagina. Foram apresentadas anteriormente boas dicas.

O problema agora se resume em fazer com que cada usuário mude a Password "default",de preferência na primeira vez que ele acessar a conta. Apresento uma sugestão a seguir.

4) Sugestões : *(Introdução do Aplicativo 'Checker')*

Tendo em vista que a grande maioria de usuários não é consciente do problema da segurança de suas Redes,a abordagem mais adequada parece ser a de se retirar dos usuários,a responsabilidade na criação de Passwords fracas . Desta forma,nossos Sistemas estariam protegidos,pelo menos de Passwords do tipo formadas por combinações do próprio nome do usuário ,e da permanência da Password "default". (como se pôde constatar nos testes feitos acima .

Esta abordagem exige a criação de um aplicativo que tenha acesso a algum tipo de Rastreador de Passwords . Com este "Software" residente no Sistema,toda e qualquer alteração (Criação e Mudança) feita sobre alguma Password,seria acompanhada da chamada a este Rastreador,que analisaria esta Password e ,dependendo do resultado,mandaria uma mensagem de que aquela Password não é adequada . Este "Software" também poderia conter dicas para se construir uma Password bem protegida

Desta forma,livraríamos os usuários do risco de serem responsáveis pela entrada de um intruso na Rede,e caberia,ao Administrador,o simples serviço de policiar a mudança periódica das Passwords (já que nenhuma Password é eternamente segura). O uso de Programas "polícia" nas Redes Unix,vem sendo insentivado mundialmente,já que tendo este método como padrão,na questão de Segurança das Redes de Sistemas Unix,estaríamos quase que aniquilando o poder de destruição dos *"hacker"* . Até agora é a melhor solução .

Conclusão

Este trabalho não traz nada de novo para os *"hackers"* mais interessados . Desta forma não estamos oferecendo nenhum segredo,mas sim, informações sobre como defender seu Sistema através de dicas para criação de uma Password segura . O Objetivo de tornar os Sistemas mais seguros ,e consequentemente livres de intrusos,depende também de uma conscientização geral neste sentido,já que um usuário mal educado põe em risco não só seus arquivos,e sua Rede local,mas como qualquer Sistema a qual ele tenha acesso .

A sugestão acima,já é padrão em vários Sistemas . Nestes,o próprio Sistema Operacional já vem com este aplicativo carregado . Como exemplo,podemos citar o AIX 3.2 que fornece dicas para se criar uma boa Password,como foi sugerido . Este Sistema,também bloqueia a conta do usuário que não acessá-la por um determinado período de tempo,aumentando assim o grau de segurança.

Após a pesquisa feita por este trabalho,muitos usuários notificaram a CAT de que várias vezes abriram suas contas e detectaram a presença de arquivos desconhecidos. É para evitar isto,e outros problemas muito mais sérios que implementaremos o Aplicativo sugerido acima (***"Checker"***) na Rede Sun do CBPF brevemente.

Bibliografia

Este trabalho se baseia no artigo ,de domínio público, "Foiling the *"hacker"* . A Survey of,and Improvements to,Password Security",de autoria de Daniel V. Klein (Carnegie Mellon University Pittsburg,PA 15217 - dvk@sei.cmu.edu +1 412 268 7791) .

O pacote contendo o Rastreador de Passwords "Crack Version 4.1" de autoria de Alec D. E. Muffett(Unix Software Engineer Aberystwyth,Wales,UK aem@aber.ac.uk or alec_muffett@hicom.lut.ac.uk) foi adquirido também em domínio público .

Fim