Breaking out of a restricted RDP session

By Wicked Clown

Bsides London 20 April 2011.

A little bit of crap about me :)

- I am Wicked Clown
- I regularly attend DC4420 (DefCON London)
- Working in the security arena for 3 years as a tech support engineer.
- Unhealthy interest in everything security related for 20 years :)
- Jack of all trades, other interests include.
  - Lock picking, Social Engineering, Exploit & Vulnerability Research, Pen testing. Anything security related!

Talk Outline

***** THIS FOR EDUCATIONAL PURPOSE ONLY!! *****

- Extended version of my lighting talk I gave at BruCON 2010.
- I got video demo's, I chicken out a live one!
- I am going to show how to fix it :(
- This is a bit of random talk (covers lots of things not just RDP)

So what have I discovered

Any one who can connect to your Terminal Server, can run and execute pretty much anything. Bypassing your Group Policy settings!! Even if you think they are restricted!

Note: Only tested on windows 2000 and 2003

Is this a security issue or not!

- Majority of people I have spoken to think this is an issue.
- Informed Microsoft – Don't seem to care.
- This is OPEN BY DEFAULT!!
- I have seen this in the wild.

Lets pop a box! - Recon

- Nmap scan the box
    - Port 3389
- Do we have an account and password?
- If no, how do we get in!
- If yes, AWESOME!!

Lets pop a box! - Username

We don’t have a username.

Most companies use the username in their email address i.e.

JD@bar.com mostly the username will be ‘JD’

Lets pop a box! - Password

* PASSWORD LOCK OUT POLICY!! *

- Brute Force or social engineer.
- Don’t need to just use TSCrack
- Check for FTP (21) or IMAP (143) services = Hydra
- Administrator DOESN’T LOCK OUT!! :)

* PASSWORD LOCK OUT POLICY!! *

Lets pop a box! – Got details

We have a valid username and password!

We log in but restricted.. And now the cool bit!! :)

DEMO!!

Lets all pray to the demo gods!!

- Show you the group policy
- Log in as user to show its restricted
- Show how to get command shell in about 5 seconds
- How to abuse this to escalate privileges
- Then how to prevent this happening

Demo

Group Policy Setup

Demo Con't

Attack – The cool bit you want to see!

Demo Cont

How to fix it – the boring bit!! ☹

Now What!!

Lets f*ck a network!

- Try the local admin password on other servers
- Check for other services running. VNC?
- Use Metasploit to route exploits through this box (Video on website)
- Upload 'Cain & Able' to sniff the network for logins / passwords

Game over man!!

Email Server

- Access anybodies email account
- Send an email from someone to their boss saying they are gay and have a crush on them.
- Search the emails for the word ‘Password’
- Use it as a spam server

Internal / External Network

- Inject malicious code into your Intranet website
- Deface or Inject code into your external website
- Attack their external resources
- Turn their machines against them
- Modifying your backups

Accounts System

- Create a phantom employee who gets paid.
- Transfer money to me or an enemy
- Publish everybody’s payslips
- Change everybody's pay
- Over charge their customers

Your Customers

- Obtain access to their networks
- Steal there information
- Block / sabotage their access to support them
- Denial of services ALL their customers

Conclusion

- Forgetting a little tick can screw you over!!
- Finding ‘features’ is not just about exploiting code
- If you get caught doing this don’t blame me

Web: www.tombstone-bbs.co.uk
Email: Wicked.Clown@tombstone-bbs.co.uk