ADVISORY CLASS : WEB PENETRATION

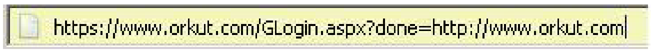
(C) ZeroKnock

REDIRECTION ATTACKS JERKED IN ORKUT : CAVEATING LOGIN ACCOUNT

ABSTRACT

There is another generic flaw is undertaken in gmail.This flaw persists in the login page and executes very definitely.In this there is specific URL request is crafted which redirects the Gmail web browser traffic to required website which a attcker wants to visit.As a result of this the connection is made through the orkut servers rather than the primary domain.The redirection is very successful and jumps to the destination.

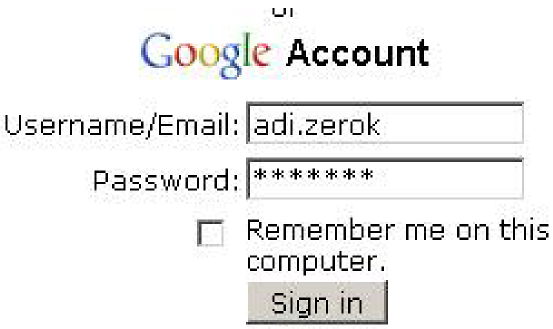
Explanation:
The Orkut login account URL is underatken as :



https://www.orkut.com/GLogin.aspx?done=http://www.orkut.com

The connection uses secure https protocol and defined Glogin.aspx but the done is the argument which redirects the acoount login to the required destination account of orkut but after the login is successful.If one manipulates the done argument and changes it another webiste the attack works very well.

The Login Works As :



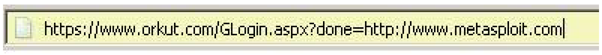
Google Account

Username/Email: adi.zerok

Password: *******

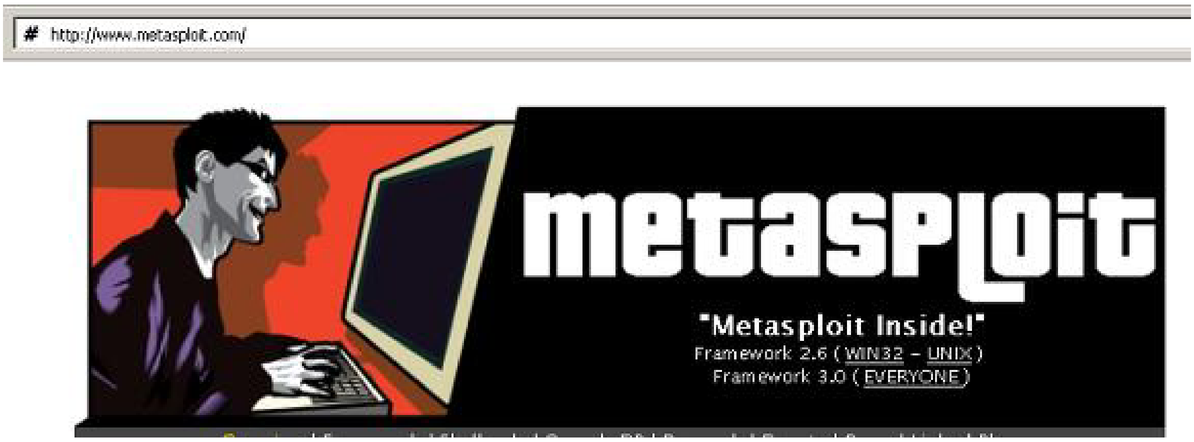
□ Remember me on this computer.

If this login is successful then we set the URL for redirection as :



https://www.orkut.com/GLogin.aspx?done=http://www.metasploit.com

So the URL is fully crafted and lets see what the result is:

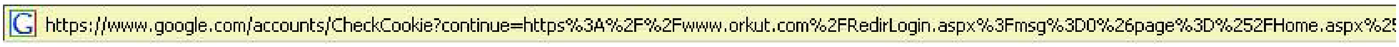


http://www.metasploit.com/

See the crafty redirection that is possible through the orkut.Attackers usually perform this to redirect traffic or apoofing their identity.This is same rogue stuff with paypal and Ebay.Oh God Whats going on!!!

There is another URL through which redirection attacks are possible.

Check this :



```
https://www.google.com/accounts/CheckCookie?continue=https%3A%2F%2Fwww.orkut.com%2FRedirLogin.aspx%3Fmsg%3D0%26page%3D%252FHome.aspx%25
```

You can see cleary the redirect argument . the redirection is possible here too.

This is doen to ensure reliablity in community caveats..

Security With Obscurity.

ADITYA SOOD (ZEROKNOCK)
INDEPENDENT SECURITY RESEARCHER
METAEYE SECURITY
HTTP://ZEROKNOCK.METAEYE.ORG

PREMATURE OPTIMISED.