<Silly Con/>

RED TEAM ENGAGEMENT

Modern World Defensive Cyber Offense

WHO THE HELL AM I ??

- A Hacker (Don’t know Bad or Good)..
- Started as Scriptkiddies .. Now Professional…future Don’t know…☺
- Freelance Penetration Tester (“Hacker For Hire“)..
- Love Red Teaming, Network Pentesting and Exploit Development and Reverse Engineering..
- Others : Painter, Biker, Sharp Shooter (Trained) and A Farmer ;)

Tweeter : @nu11_v0id
Facebook: fb.com/lovelyindranil
E-mail : indranilbanerjee21@gmail.com

MODERN WORLD CYBER SECURITY

"Internet was never designed to be the backbone of a global economy"

- Shift from a Deterministic to a Probabilistic Approach
- Scale the Cost of Operating a Resilient Cyber Infrastructure
- Take the Next Step: Artificial Intelligence
- Skill Development and Research

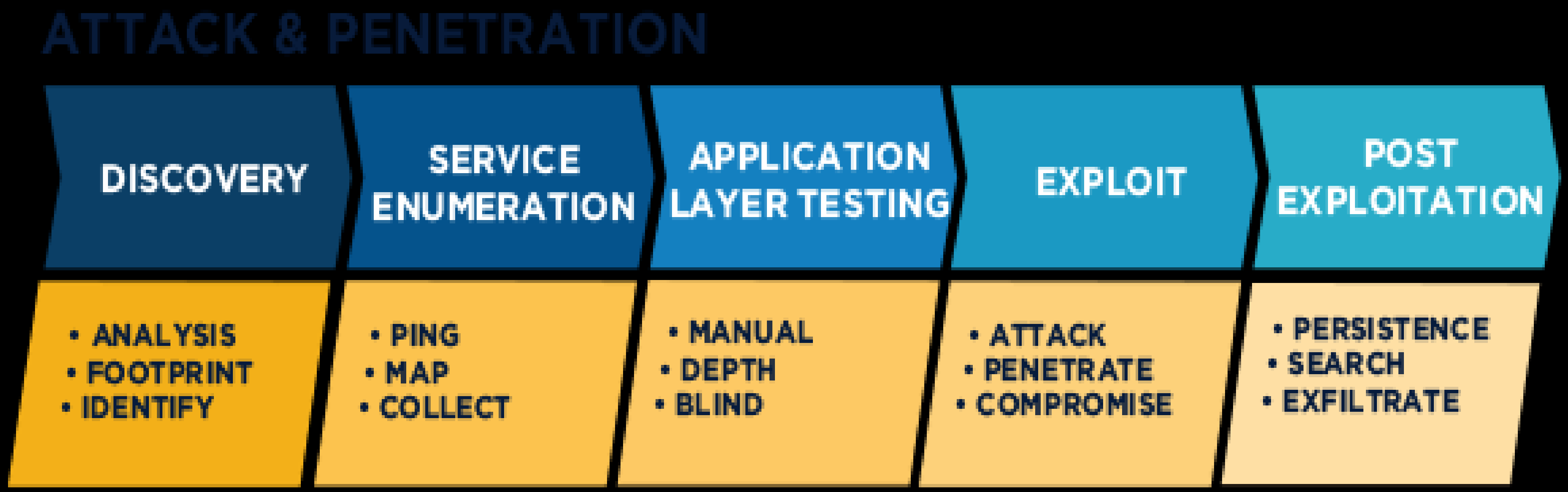
MODERN WORLD CYBER SECURITY RISKS

- Identity Risks
- Risks in Related to Web Applications
- Risks in IoT
- Infrastructure Security Risks
- Cyber Wars (Internet Gang Wars)
- Sponsored Cyber Espionage
- StartUps are at Risks
- Insider Threats
- And so on…….

http://map.norsecorp.com/

WHAT IS RED TEAM PENTESTING ?

RedTeam Pentesting offers individual penetration tests, short pentests, performed by a team of specialized IT security experts. Hereby, security weaknesses in IT systems (e.g. networks, applications or devices) are uncovered and can be remedied.

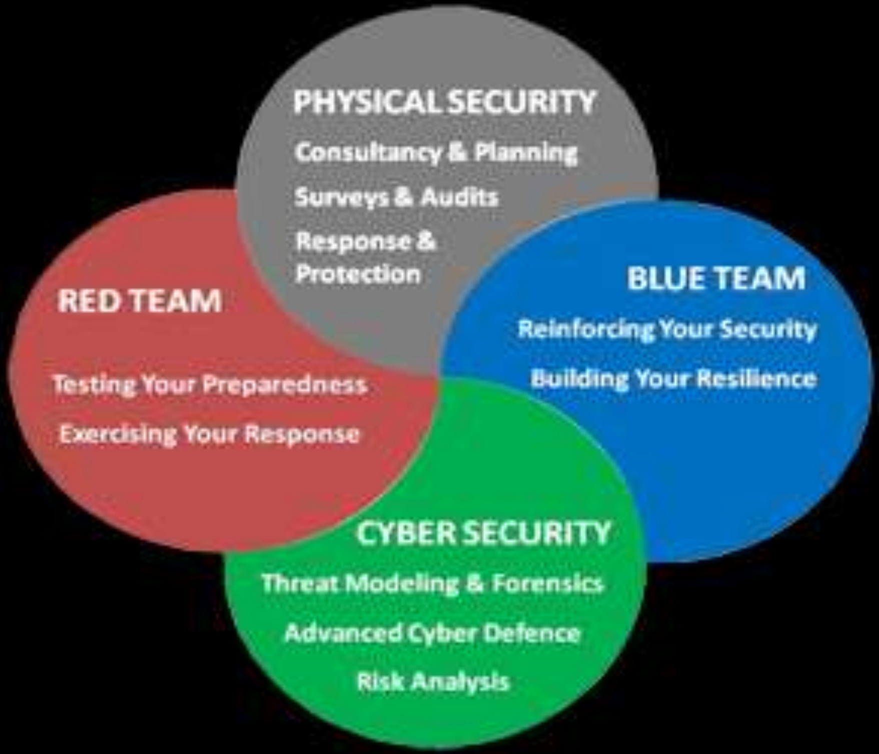


ATTACK & PENETRATION

DISCOVERY	SERVICE ENUMERATION	APPLICATION LAYER TESTING	EXPLOIT	POST EXPLOITATION
• ANALYSIS • FOOTPRINT • IDENTIFY	• PING • MAP • COLLECT	• MANUAL • DEPTH • BLIND	• ATTACK • PENETRATE • COMPROMISE	• PERSISTENCE • SEARCH • EXFILTRATE

Why You Should Conduct ?

“How Do You can put up a fight if you have never taken a punch”



Real world Testing to test you much secure your infrastructure is against Highly Skilled, Funded and Motivated Cyber Attacks

A Pentesting that covers all type of testing

DEMO

How To Red Team Engagement?

Outside of The Box Thinking

Think like a "Sophisticated Attacker" and try to dig out the jewels (Sensitive Information) out from the organization to show the risks involved with their defense. Follow through different types of attack simulations to find the real value data and information possible.

TOLD YOU
TO
THINK NOT
TO
CRAP

TECHNOQUES & TOOLS

Physical Security Testing

- Lock picking
- RFID Card cloning
- Lan to VPN
- Many others…

External & Internal Network Exploitation

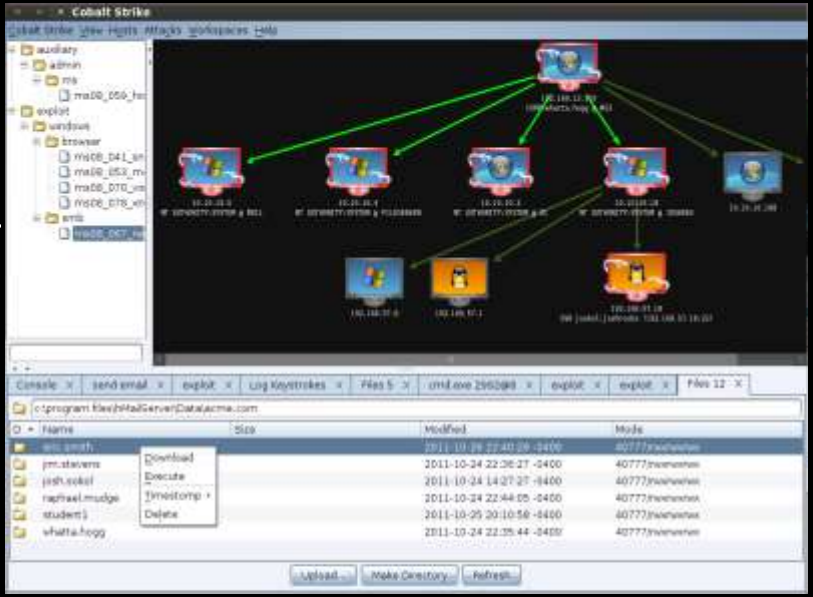
Techniques & Tools

- Remote Exploitation
- 0-day attacks (Very Rear)
- Attacking through Rouge AP
- Attack on wireless Infrastructures to ga
  access
- Attacking through Bluetooth
- Browser based Attacks
- Metasploit Browser based Exploitations
- Java Applet Attacks
- HTA Attacks
- DNS Hijacking and Network Tunneli

AIRCRACK-NG

metasploit

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS



c:\program files\hMailServer\Data\acme.com

Name	Size	Modified	Mode
eric.smith		2011-10-28 22:40:28 -0400	40777/rwxrwxrwx
jim.stevens		2011-10-24 22:36:27 -0400	40777/rwxrwxrwx
josh.sokol		2011-10-24 14:27:27 -0400	40777/rwxrwxrwx
raphael.mudge		2011-10-24 22:44:05 -0400	40777/rwxrwxrwx
student1		2011-10-25 20:10:58 -0400	40777/rwxrwxrwx
whatta.hogg		2011-10-24 22:35:44 -0400	40777/rwxrwxrwx

ARMITAGE
FAST AND EASY HACKING

BeEF

Web Application Attacks

- Attacks against organizations CMS
- Attacking Webmail to get internal user information
- Attacking Internal Mail Servers
- Hijacking Session Cookies
- Embedding Reg Key
- And Many more…..

Social Engineering Attacks

- Most Successful one
- Social Engineering Toolkit (SET)
- Metasploit
- Maltego (Information Gathering)
- Google Hacker Database
- Etc……

Case Study

Indian Organizations at Risk

- Increase rate of Cyber Attacks against Indian Organizations
- Poor Cyber Defense
- Lack of Cyber Awareness
- Huge gathering of PentestPuppies
- Poor balancing between Security and Business
- Unsatisfied workforce → Internal Threat
- And many more… (What you Say..!!)

StartUps are at Risk

- High Quality Intellectual Property
- Big Potential (Not Aware of Security) → Theft → Failure
- High Competition → ingress monitoring → Theft

Mitigations

- Cyber Awareness from the Elementary Level of Education
- More Budget allocation on Security.
- Getting rid of PenTestPuppies ;)
- Threat Mitigation Workforce
- Proper Security Education for Staffs and Executives

[Left for you and thing You wanna add]

Share Your Experience

Best Story will get a **RedTeam Tool** as a Gift !!!

I AM DONE !!

Q & A