RMAR Certified Cyber Security Expert (RCCSE)
RMAR Dizi Securities
(A Training Division of RMAR Technologies Pvt. Ltd.)

,

Course Duration: 80Hrs.
Course Fee: INR 7000 + 1999 (Certification Lab Exam Cost–2 Attempts)

Course Module:

1. **Introduction to Ethical Hacking**
2. **Footprinting**
    a. SAM Spade
    b. Nslookup
    c. Nmap
    d. Traceroute
3. **Scanning**
    a. Port Scanning
    b. Banner Grabbing
4. **Enumeration**
    a. **Attacking Null Sessions**
        i. DumpSec
        ii. Winfo
        iii. Sid2User
        iv. NBTenun
    b. **Enumerating Windows Active Directory Via LDAP, TCP/UDP**

5. **System Hacking**
    a. **Using Live Operating Systems**

i. Back|Track
ii. OPHCrack
iii. Trinity Rescue Kit
iv. Offline Password Cracker
v. Konboot
vi. Countermeasures

6. **Trojans & Backdoors & Countermeasures**
7. **Network Sniffing Attack**
    a. Dsniff
    b. Ettercap
    c. SSLStrip
    d. Cain & Abel
    e. Wireshark (For Packet Analysis)
    f. Countermeasures
8. **Penetration Testing**
    a. The Phases of the PTES
    b. Types of Penetration Tests
        i. Overt Penetration Testing
        ii. Covert Penetration Testing
9. **Metasploit**
    a. **Terminology**
    b. **Metasploit Interfaces**
        i. MSFConsole
        ii. MSFCli
        iii. MSFGui

iv. Armitage

c. Metasploit Utilities

i. MSFpayload
ii. MSFencode
iii. Nasm Shell

d. Metasploit Express & Metasploit Pro

e. **Intelligence Gathering**

i. Passive Information Gathering
ii. Active Information Gathering
iii. Targeted Scanning

f. **Vulnerability Scanning**

i. Scanning with NeXpose
ii. Scanning with Nessus

g. **Begin with Exploits**

i. Exploiting your First Machine
ii. Exploiting an Ubuntu Machine

h. **Meterpreter**

i. Exploiting Windows XP Machine
ii. Dumping Usernames & Passwords
1. Pass the Hash
2. Privilege Escalation
3. Token Impersonation
4. Using ps
5. Pivoting onto other Systems

i. **Using Meterpreter Scripts**

i. Migrating a Process
ii. Killing Antivirus Software
iii. Obtaining System Password Hashes
iv. Viewing All traffic on a Target Machine
v. Scraping a System
vi. Using Persistence

j. **Avoiding Detection**
   i. Creating Stand-Alone Binaries with MSFpayload
k. **Evading Antivirus Detection**
   i. Encoding with MSFencode
   ii. Multi-encoding
l. **Custom Executable Template**
m. **Launching a Payload Stealthily**
n. **Exploiting Using-Client Side Attacks**
   i. Browser Based Exploits
   ii. Exploring Internet Explorer Aurora Exploit
   iii. File Format Exploits
   iv. Sending the Payload
o. **Metasploit Auxiliary Modules**
   i. Auxiliary Modules in Use
   ii. Anatomy of an Auxiliary Module
p. **The Social-Engineer Toolkit**
   i. Configuring the Social Engineer Toolkit
   ii. Spear-Phishing Vector
q. **Using Stdapi**

r. **Meterpreter Extensions Stdapi & Priv**
s. **Metasploit Database Integration & Automation Exploits**
t. **Backdoors & Rootkits**
u. **Countermeasures**

10. **Snort - IDS/IPS Implementation**
11. **Wireless Hacking**
    a. Understanding different IEEE Standards of Wireless
    a. WEP Cracking
    b. WPA-Psk Cracking
    c. WPA2-Psk Cracking
    d. Enterprise Wifi Cracking
    e. Caffe Latte Attack
    f. Countermeasures
12. **Website Penetration Testing**
    a. SQL Injection Attack
        i. Using manual query based SQL Injection
        ii. Using Havij
        iii. Using SQLMap (Back|Track)
    b. Cross Site Scripting (XSS) Attack
        i. Persistent XSS
        ii. Non-Persistent XSS
        iii. Reflected XSS
        iv. Post XSS
        v. LFI & RFI
        vi. Bypassing Filters

c. Shell Attack
    i. Gaining Server Access
    ii. Rooting Linux Server & getting meterpreter session on windows server
    iii. Mass Website Attack
    iv. Botnets
    v. Denial of Service (DoS) Attack
    vi. Distributed Denial of Service (DDoS) Attack
    vii. E-mail Spoofing
    viii. E-mail Bombing
    ix. Mass Mailing
d. Countermeasures
e. OWASP

13. **Linux Hacking & Countermeasures**
14. **Router Hacking & Countermeasures**
15. **Reverse Engineering**
16. **IT Laws & legal working layout of Ethical Hacker**

LAB TEST