SANDEEP SAINI

Security Researcher and Penetration tester

FREELANCER

PROGRAMMER

PENETRATION TESTER

SECURITY RESEARCHER

: programmingethicalhackerway@gmail.com

: +91 96507 57145

Hindi (Fluent) *English (Conversational)*

PROFESSIONAL SKILLS

- ***Network penetration testing*** 98%
- ***Source code reviews*** 97%
- ***Exploit and Shellcode Development*** 60%
- ***Penetration testing*** 99%
- ***Web penetration testing*** 98%
- ***Server Hardening*** 95%
- ***Reverse Engineering*** 65%
- ***Malware Analysis*** 70%

PROFILE

Age	24
Address	Delhi,India
Freelancer	2013-present

EDUCATION

- **Central Board of Secondary Education (CBSE), New Delhi**
  - Class Xth-XIIth (2008-2010)
- **Netaji Shubhash Institute of Technology, New Delhi**
  - B.E. in Electronics and communication (2011-2015)

SOCIAL LINKS

- Python based Information security project: https://github.com/SandeepSainiProgrammer
- Blog on Vulnerability Assessment and Penetration Testing: http://systempenetration.blogspot.in/
- Blog on Programming(C/C++, Assembly, Python) http://programmingethicalhackerway.blogspot.in/
- Blog on latest 0-day vulnerabilities and exploits: http://0dayexploitcode.blogspot.in/
- YouTube channel on Web application and System Security: https://www.youtube.com/channel/UC1Q6q7yoUYbi0vFdhletPuA/videos
- Linkedin Profile: https://www.linkedin.com/in/sandeep-saini-programmer/

EXPERIENCE

1 ***Network penetration testing (2013-persent):***

Do both manual and automated network penetration testing.
Approach for Manual Network Penetration Testing: Manually check for IDS/IPS rules, network and server's Services, Networks switch and Router's configuration, VPN, Firewalls rules, Anti-virus, Authentication, Authorization etc.
Approach for automated network penetration testing: Following tools use to perform the network penetration testing:

Nessus(2013-persent):

Use nessus to identify the network vulnerabilities (including IPv4/IPv6/hybrid networks).
Un-credentialed vulnerability discovery And Credentialed scanning for system hardening and missing patches.
Scan Network devices: firewalls/routers/switches(Juniper, Check Point, Cisco, Palo Alto Networks), printers, storage.
Scans the configuration of cloud applications like Salesforce and cloud instances like Amazon Web Services, Microsoft Azure etc.
Use nessus to detect viruses, malware, backdoors, hosts communicating with botnet-infected systems, known/unknown processes, web services linking to malicious content
Use nessus for various softwares like Virtualization(VMware ESX, ESXi, vSphere, vCenter, Microsoft, Hyper-V, Citrix Xen Server);Operating systems(Windows, Linux, Solaris,FreeBSD, Cisco iOS); Database(Oracle, SQL Server, MySQL,PostgreSQL, MongoDB) Follow PCI DSS requirements for internal vulnerability scanning

Metasploit(2013-peresent):

Use Metasploit to find, exploit, and validate network and system vulnerabilities. Manually run exploit (choose and configure an exploit) to run against a target.
Use metasploit to executing exploit code against a remote target machine. Use various techniques to evade antivirus, find weak credentials, and pivot throughout the network.
Use metasploit for exploitation, post-exploitation reconnaissance(record a user's keystrokes, mine password hashes, root around in the file system , use command line commands, escalate privileges, take snapshots or video with a webcam), token manipulation, social engineering attacks etc.

Armitage(2013-persent):

Use armitage to visualizes targets, recommends exploits, and exposes the advanced post exploitation.
Use armitage to recommends and run active checks to all the exploits which will work.

Nexpose(2013-persent):

use nexpose to scan a network for vulnerabilities.
Use various templates like Internet DMZ audit; Microsoft hotfix; Full audit; PCI internal audit; Penetration test; Safe network audit; Web audit etc

NMAP(2013-persent):

Use NMAP to understand network topology and find which machines are connected to it, which versions of operating systems they are running, which ports they have open, and what vulnerabilities might exist.
Nmap used to scan networks to find out which services and hosts are listening and may be vulnerable to compromise.
Use Nmap Scripting Engine (NSE) to run scripts to scan for well-known vulnerabilities, allowing find any known vulnerabilities in infrastructure.
Uses different techniques to perform scanning including TCP SYN scan; TCP connect scan; UDP scans; Xmas scans; zombie scan etc

Maltego(2013-persent):

Use maltego querying various public data sources and graphically depicting the relationships between entities such as people, companies, web sites, and documents.
Use maltego gathering info on all the subdomains, the IP address range, the WHOIS info, all of the email addresses, and the relationship between the target domain and others.
Use maltego to finding information on a particular organization

OpenVAS(2015-2017):

Use OpenVAS to perform comprehensive security testing of an IP address.Audit the security of an internal corporate network and find vulnerabilities.
Use various scan type like Full Scan(full test of network, server and web application vulnerabilities) ; Web Server(Scan a more focused test for web server and web application vulnerabilities) ; WordPress Scan(testing for known WordPress vulnerabilities and web server issues); Joomla Scan(testing for known Joomla vulnerabilities and web server issues) etc

Wireshark(2013-2015):

Use wireshark to capturing packets, filtering them, and inspecting them.
Use to analyze the structure of different network protocols.
Use Display filters to filter and organize the data display.
Use to troubleshoot network problems Use wireshark to track network resources, see potential saturation points, track user activity, insure connectivity.

2 *Web Penetration testing (2015-Persent)*

Do web application penetration testing with the standard methodology like OWASP top 10, SANS top-20 etc. Perform both manual and automated penetration testing for vulnerabilities like Injection flaws(Such as SQL injection, NoSQL injection,OS injection,LDAP injection etc); Broken authentication; Sesitive data exposure; XML External Entities (XXE);Broken Access Control; Security Misconfiguration Cross-Site Scripting (XSS) ; Insecure Deserialization ; Using Components with Known Vulnerabilities ; Insufficient Logging & Monitoring.

Approach for Manual Web-Application Penetration Testing:

Conduct manual testing with following controls:
* Configuration and Deployment Management Testing
* Identity Management Testing
* Authentication Testing
* Authorization Testing
* Session Management Testing
* Input Validation Testing
* Testing for Error Handling
* Testing for weak Cryptography

Approach for automated web penetration testing:

Following tools used for automated penetration testing:

Burp-suite(2015-persent):

Configures browser to route traffic through the proxy which then acts as a sort of Man In The Middle by capturing and analyzing each request and response to and from the target web application
Use Burp Suite for Web applications to check any input from the user to ensure it is in the right format.
Use various burp-suite features like HTTP Proxy(used for interception, inspection and modification of the raw traffic passing in both directions) ; Scanner(used for performing automated vulnerability scans of web applications) ; Intruder(can test and detect SQL Injections, Cross Site Scripting, parameter manipulation and vulnerabilities susceptible brute-force attacks) ; Sequencer(Used to analyzing the quality of randomness in a sample of data items and used to test an application's session tokens or other important data items that are intended to be unpredictable, such as anti-CSRF tokens, password reset tokens, etc.); Spider(used to automatically crawling web applications) ; Repeater(used to manually test an application by modify requests to the server, resend them, and observe the results) ; Decoder(Use to decode and encode strings to various formats i.e. URL, Base64, HTML, etc.) ; Extender(used to load Burp extensions, to extend Burp's functionality using own or third-party code)

Acunetix (2015-persent):

Use Acunetix Vulnerability Scanner to scans web applications, finding all known vulnerabilities like SQL Injection, XSS, XXE, SSRF, Host Header Injection etc.
Use Login Sequence Recorder for automatic scanning of complex password protected areas.
Use various Scan Types to scan the application like Full Scan; High Risk Vulnerabilities; SQL injection; Cross-Site Scripting (XSS) etc.

OWASP-ZAP(2017-persent):

Use OWASP ZAP for finding vulnerabilities in web applications.
Use spider to crawl the application and automatically passively scan all of the pages discovered.
Use the active scanner to attack all of the pages discovered by spider.
Use various OWASP ZAP features like Intercepting Proxy; Automated Scanner; Passive Scanner; Brute Force Scanner; Fuzzer; Port Scanner; Spider; Web Sockets; REST API etc.

Netsparker (2015-persent):

Use Netsparker finds and reports web application vulnerabilities such as SQL Injection and Cross-site Scripting (XSS); command injection; directory traversal etc. on all types of web applications
Use various authentication methods like Basic Authentication; Form Authentication; NTLM Authentication; Digest Authentication; Kerberos Authentication to test in depth.
Use netsparker to scan various types of web services like SOAP 1.1 and 1.2 ; REST API .

3 *Exploit Development and Shellcode Development (2013-2015):*

Have intermediate experience in exploit development for windows and linux:
Use various techniques to exploit buffer overflow vulnerability like stack base exploitation; heap based exploitation etc.
Bypass windows mechanism protection like bypass /GS; bypass SafeSEH; Bypass ASLR; Bypass DEP; Bypass SEHOP etc.
Develop user space shellcode like port bind shellcode; reverse shellcode; staged shellcode; egg-hunt shellcode etc.
Design shellcode functionality like File transfer; download and execute; process injection shellcode etc.

Tools used in exploit development:

GDB debugger :

Use GDB to define of application for vulnerability development.

Immunity debugger:

Use Immunity debugger to find CPU instructions, Register address; Stack location; memory dump .

IDA Pro:

Use IDA pro to define and reverse the code while finding bug and identify the vulnerabilities.Use IDA pro to graphical representation of the control flow graph.

4 *Reverse engineering and Malware analysis (2013-2015):*

Have 2 years of experience in reverse engineering and malware analysis:

Hands on experience in Intel x86: Architecture, Assembly.
Use reverse engineering analysis (Static analysis and Dynamic analysis) to decompilation of application and find software vulnerabilities.Analysis the header of binary program for malware analysis.
Analysis PE File Format to understand How windows loader loads the executable in memory; How loader build the import and export table for a module in memory; From where to start the execution or Address of entry point.
Experience with packer, crypters.

Tools:

PEview:

use PEview to determining basic PE information

CFF Explorer:

Use CFF explorer to file identification, address conversion, dependency scanning, and the ability to add imported functions to a PE.

Hex editor Neo:

Use hex to searching for specific bytes, saving sections of a binary to disk.

IDA pro:

Use to List of all locations that refer to a particular piece of data and List of all locations that call a particular function.

5 *Penetration testing (2013-persent):*

Follow the standard methodology to perform the penetration testing:

Information gathering:

In this step, gather the information about the target like whois; port scanning; technology used; services identification; sensitive data etc.

Tools:

NMAP, Maltego, Whois, Wireshark, theHarvester , Dmitry,Dig, GHDB etc.

Vulnerability Assessment:

In this step, find the vulnerabilities existing in the target.
Tools: Nessus, Netsparker, Nexpose, Acunetix, Burp-suite, openVAS, IBM Appscan,HP fortify.

Exploitation:

in this step, exploit the vulnerabilities.

Tools:

Metasploit, SQLMAP, Burp-suite, Armitage, THC-hydra, etc.

Reporting:

The final step is reporting. Simulate all things in the report for both technical and non-technical persons.

6 *Source code reviews (2017-persent):*

Perform source code reviews for .NET and PHP language:

Perform vulnerability analysis on .net based websites using standard methodology like OWASP top 10, SANS 25 etc.
Perform manual and automated source code reviews for various web based security vulnerabilities like SQL injection, Cross site scripting (XSS), CSRF, RFI, LFI, Authentication bypass etc.
Use HP fortify and IBM Appscan source tool to analysis source code.
Analysis about false positive results generated by the scanner tools like HP fortify, IBM Appscan source.
Use Burp-suite in manual web pen testing like session token analysis, SQL injection payload, Check token strength etc.
Suggest coding mitigation to the web-developers.

CERTIFICATION:

~~→ CEH~~

~~→ OSCP~~

~~→ CISSP~~

~~→ CCNA~~

› **Believes in practical knowledge rather than collecting certificate.**

STRENGTH:

- Efficient
- Punctual
- Quick learner
- Proactive