VAPT – Assessment & Testing

BE THE BENCHMARK

CERTIFICATION & BUSINESS ENHANCEMENT SOLUTIONS

WHEN YOU NEED TO BE SURE

SGS

WHAT IS VAPT?

- A process to evaluate and review key systems, networks and applications
- To identify vulnerabilities and configuration issues that may put the organization at risk of being breached or exploited
- Effective in identifying vulnerabilities, but it cannot differentiate between exploitable vs non-exploitable vulnerabilities

WHAT IS PENETRATION TESTING?

- Goal-driven test focused on identifying all possible routes of entry an attacker could use to gain unauthorized entry into the target
- Identifies the potential damage and further internal compromise an attacker could carry out once they are past the perimeter.
- Proof of concept strategy to investigate, exploit and validate the extent of the identified vulnerability

TEST TYPE

Black Box Testing

- Testing from an external network with no prior
- knowledge of the internal network and system

White Box Testing

- Test being performed from within the network
- Prior knowledge of the network, architecture and
- system.

Grey Box Testing

- Testing from an internal or external network
- Partial knowledge of the internal network and system
- Combination of both white and black box testing

TEST TYPE

Network Vulnerability Assessment & Penetration Testing

- Internal & External IPs
- VoIP & Cloud ;Telephony
- Devices – Firewall, Switches, Routers , etc.
- AWS Cloud

Configuration Review

- AWS Cloud Assessment
- Devices – Firewall, Switches, Routers, etc.

SGS

WHY VAPT?

Mobile Insecurities

Scary facts to encourage you to practice cyber hygiene.

41% of people globally can't identify a phishing email

In 2017, there were 8.9 incidents of identity theft per 100,000 Canadians (that's quadrupled since 2010)

iPhone users are 2x more likely to experience mobile phishing attacks than Android users

80% of mobile fraud is done through apps

Top 2 app categories with the most malicious apps:

- Lifestyle apps (27%)
- Music and audio (20%)

25% of all web-based mobile phishing attacks come from games

CYBERSECURITY MYTHS FOR SMES

- **I have a firewall, so I'm safe from attacks**

  Hackers understand strategies adopted by a firewall quite well. Disrupting codes and exploiting basic IT oversights to gain access to your system is easy.
  While most cyber security threats are avoidable, your organizations can not rely solely on firewalls for protection.

- **I use HTTPS, so my site is secure**

  HTTPs safeguards the transmission of information from source to destination. This is web security at a minimal.
  It does not block attacks like DDoS, brute force, injections, etc.
  There is also the issue of organizations using fake SSL certificates, resulting in their organization being compromised

- **SMEs are safe because they are not worthwhile targets**

  SMEs are considered to be low hanging fruits for hackers because so many do not take security seriously.
  One of the most popular attacks that hackers use against SMEs is ransomware.

WHY DO SMES NEEDS VAPT?

- **Basic security measures are not enough.**
  Firewalls or anti-virus solutions are not sufficient to protect against attacks.

- **Security budget**

  Unlike MNCs, SMEs do not have the budget to implement everything.
  There is limited or no resource for security expertise.
  What VAPT adds value to is to streamline what is needed for the organization.

- **Reputation**

  Potential clients or business partners will feel insecure on collaboration.
  Contributing factors can be issues like safeguard of important data.

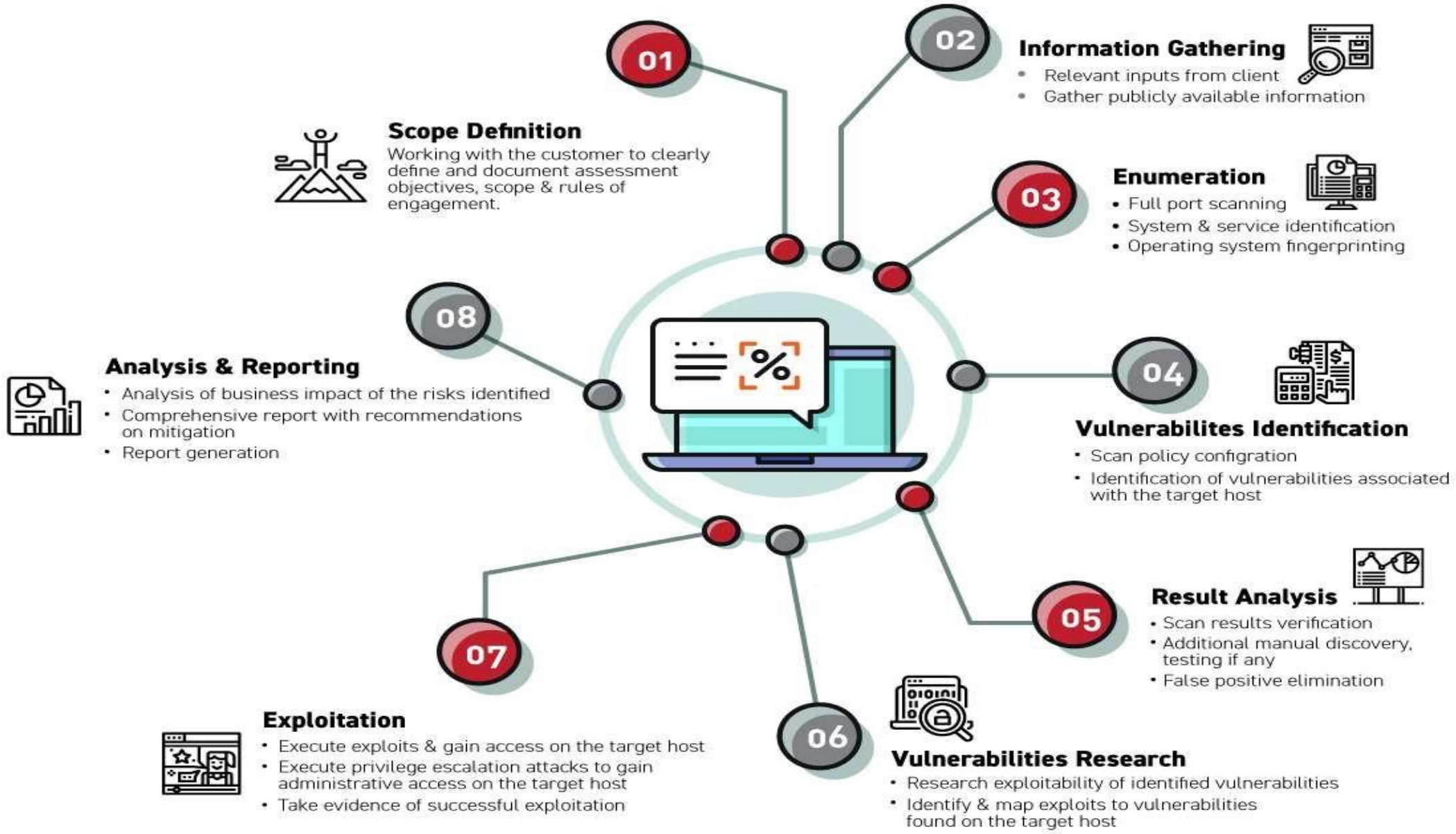
- **SMEs also lose out on potential/existing business.**

  Compared to SMEs, larger organizations have a much greater potential to survive an attack due to the help of current investors and existing large clients. (E.g. Sony (04/2011) survived through the attack.)

OBJECTIVES & PROCEDURES

- **Objective -** The scope will be scanned and tested for vulnerabilities using a wide variety of tools and techniques.
- The tools and techniques used will be consistent with current industry trends regarding exploitation vulnerabilities.
- **The tools and procedures are:**
- Threat and attack vectors
- Combination of vulnerabilities exploited in a particular sequence
  Business and operational impact of attacks
- Efficiency of the client’s network and environment to detect and respond to attacks
- Areas of focused investment to reduce or mitigate risks

OBJECTIVES & PROCEDURES



METHODOLOGY

- **D**iscovery - aims at identifying all potential assets for investigation. The information gained through the discovery process creates a road map for the investigation module.
- **A**nalysis - utilizes the list of assets from the discovery process and thoroughly examines them for potential vulnerabilities. The raw data resulting from the investigation must be analyzed and verified.
- **V**alidation - tests vulnerabilities to ensure that all false positives and inaccuracies are removed from the raw investigation data. This often-neglected step ensures accuracy, painting a nearly complete picture of the security posture.
- **E**xploitation - involves the in-depth analysis and execution of advanced testing techniques against all verified vulnerabilities. This effort completes the security picture and provides the information necessary to fully mitigate the observations.
- **R**eporting - provides an overview of the assessment methodology, vulnerability and threat assessment observations, recommendations and corrective actions and a copy of all data collected.

METHODOLOGY

Phase 1– Reconnaissance

- Reconnaissance is an information gathering phase for the target IP address or IP addresses range in the scope of penetration test.
- Our team examined the target by passive techniques such as
- Internet Service Registration – The global registration and maintenance of IP address information.
- Domain Name System – Local and global registration and maintenance of host naming.
- Search Engines – Specialist retrieval of distributed material relating to an organization or their employees.
- Email Systems – Information contained within and related to emails and email deliver processes. Mainly information disclosed via “Contact Us” features.
- Website Analysis – The information intentionally made public that may pose a risk to security.
- Observations of reconnaissance whether technical or non-technical in nature, can be used against target IP address to plan further attack scenarios. This phase uses various search engines, mailing groups, online forums, collaboration sites etc. for collecting information. A subset of the same is –
- Search engines such as Google, Yahoo etc.
- Zone-h (information related to compromise disclosure).
- GHDB (Google Hacking Database leverage to an external attacker).

METHODOLOGY

Phase 1I– Port Scan

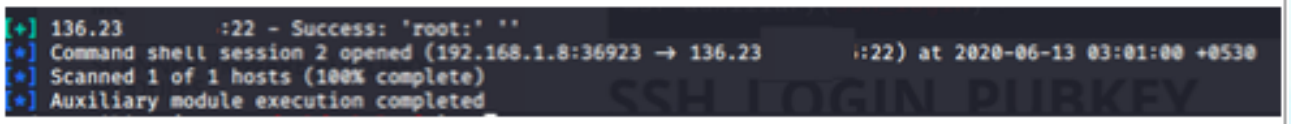
- Port Scans are attempts to connect to ports corresponding to services on the assessed hosts. By scanning ports which are available on the hosts, potential weaknesses on them can be further exploited.
- Any ports that are found visible on the hosts should be verified if they are supposed to be opened there. Unexpected open ports should be closed. The firewall should also be checked if the listening ports on the hosts should expose to the Internet or to the internal networks. It is recommended to remove any unnecessary services and implement firewall rules to prevent exposure of any legitimate services that are not meant for the Internet.

- Ports on which the connection attempts were made are shown below. The table consists of host IP addresses, protocol types, port numbers and the probable services. It is recommended to remove any unnecessary ports/services as identified below.

METHODOLOGY

- **Phase III – Observations**

- This phase has been completed successfully. The vulnerabilities which were observed during the external network penetration testing are listed below:

SSH User Login Bruteforced	
Port	TCP 22
Observation	One or more valid SSH user logins have been found through bruteforcing. An account on a router firewall or other network device has a default null blank or missing password
Risk Level	Critical
Affected Resources	127.0.0.1
POC	
Risk Mitigation	.Change the user passwords so that they are difficult to guess. Restricting management access to only trusted management networks and hosts will help mitigate this issue. The attack can only be executed from a location where a legitimate management login would be permitted.
Reference	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7755 https://www.securityfocus.com/bid/79626
CVSS Base Score	10

METHODOLOGY

- **Phase III – Observations**

TLS version 1.0 and 1.1 protocol detection	
Port	TCP 443
Observation	The remote service encrypts traffic using an older version of TLS.
Risk Level	Medium
Affected Resources	115.0.0.1
POC	scan report for 115. .vsnl.net.in (115. Host is up (0.0078s latency). PORT STATE SERVICE 443/tcp open https | ssl-enum-ciphers: | TLSv1.0: | ciphers: | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp521r1) - A | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp521r1) - A | TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A | TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A | compressors: | NULL | cipher preference: server | warnings: | Weak certificate signature: SHA1 |_ least strength: A
Risk Mitigation	Enable support for TLS 1.2 and 1.3- and disable support for TLS 1.0 & 1.1
Reference	https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00 http://www.nessus.org/u?c8ae820d https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00
CVSS Base Score	6.1

METHODOLOGY

Phase IV – Exploitation

- Our assessor observed few vulnerability which can be exploited within a given period and based on that determined that these vulnerabilities can affect confidentiality or integrity of critical information. The necessary information was gathered for the identified vulnerabilities.

Sr. No.	Attack Vectors	No. of Observations
1	Operating System Vulnerabilities	Fifteen Vulnerabilities Observed
2	Service Mis-configuration	Twenty-Five Vulnerabilities Observed
3	Network Mis-configuration	Nine Vulnerability Observed
4	Web Interfaces Discovery	Fourteen Vulnerabilities Observed
5	Common ports used by Backdoors / Viruses / Worms	No Vulnerabilities Observed
6	DNS Recursion / Zone Transfer / Poisoning	No Vulnerabilities Observed

Visit Here for More Information:

https://onlineservices.sgs.com/cyber-security/ept-external-penetration-testing/DIDTP3

Contact Us: Email: Cbe.Marketing@sgs.com Toll Free No: 1800 10 33449