Enciphers

PENETRATION TESTING METHODOLOGY

To defeat an attacker in his/her own game, you need to think like one. We at **ENCIPHERS** follow a hacker's perspective while performing any penetration test. In general terms, the security teams start with looking for any easily exploitable vulnerability in services or network which may give access to the internal network or different sensitive data.

Below are the major steps which we perform during each penetration test:

PHASE I – "KNOWING THE TARGET"

WHAT THIS PHASE IS ABOUT?

It is important that the penetration tester is very clear of the domains he/she is allowed to test as violation of this can also lead of several issues. Also, this phase is quite essential because a tester needs to understand how the application works in order to break into it. It's always better to check out each and every feature of the application before proceeding to test.

How ENCIPHERS perform this phase?

We strictly stick to the target details provided in the penetration test approval document. If the client has given specified targets, then we are sticking to it (for example if the client has given the project for testing domains like authors.target.com or blog.target.com then you can't test the domains sells.target.com as it is not in the target scope).

In case of the targets which have "**All-domains**" in their scope (for example ***.target.com**), we need to determine all the available domains. This is where we start with ***Subdomain Enumeration***. There are different tools for subdomain enumeration which you can find in the tools section below. This will help the penetration tester discover all the domains on which he is allowed perform the test.

Once all the subdomains are noted/discovered, we perform an intense **Nmap scan** on the target to find which ports and services are in use, which operating system is being used by the target and thereby make a list if some unnecessary ports are open which are then tried for exploitation in the later phases.

Since this is the information gathering phase, one should think like a Developer and have a thought approach of how the Developer tried to make the application work. This helps in the later phases.

TOOLS WE GENERALLY USE IN THIS PHASE:

- Target Scoping:
  - Subdomain enumeration
    - Enciphers custom scripts for subdomain enumeration
    - Subbrute
    - Sublist3r
    - Google Dorks.
- Port/Service Scanning:
    - Nmap
    - Nmap script Engine (NSE) scripts.
    - Masscan

PHASE II – "AUTOMATED VULNERABILITY SCANNING"

WHAT THIS PHASE IS ABOUT?

In this phase, we use different commercial and open-source software to identify missing patches, insecure services, default credentials, and OWASP TOP 10 vulnerabilities (i.e. SQL Injection, Cross-Site Scripting, Access Flaws, Authentication attacks, Sensitive Data Exposure, etc.) This phase helps us to have a rough knowledge of the different flaws that might be persisting in the application as of now. Also, this helps as a great starting point because you need to just wait for the tools to do their work and again gain lots of information about the application's security.

How ENCIPHERS perform this phase?

The security team at ENCIPHERS use different tools to perform automated testing of the target. These tools are able to scan the whole scope at once for all the available vulnerabilities. We use Burpsuite Pro for both passive and active scanning of the target. Nessus is also used during this phase to get an idea about the different vulnerabilities in the application. The vulnerabilities if found are then validated in the next phase of manual testing which leads to the elimination of any false-positives found during the automated testing and discovery of more critical vulnerabilities.

TOOLS WE GENERALLY USE IN THIS PHASE:

- Burp suite Pro
- Nessus
- Acunetix
- Nmap
- Nmap script Engine (NSE) scripts.

PHASE III - “MANUAL VULNERABILITY SCANNING"

WHAT THIS PHASE IS ABOUT?

This is the best part of the whole game. Manual testing is necessary because there is a huge list of vulnerabilities like IDOR, privilege escalations, logical vulnerabilities etc. which scanners are not able to discover. Also many a times you will need to manually validate the findings obtained from automated testing. This is the phase where one needs to think like a hacker instead of a developer. You need to think of breaking into the application and get hands on any sensitive information. Of course, these are all done ethically keeping in mind if the client wants us to dig deeper or if we are allowed to do stress testing like DoS and DDos attacks.

How ENCIPHERS perform this?

Inserting different **payloads** and making sure each field is checked for different kinds of vulnerabilities is the main step for manual testing. Different **custom written scripts** are also used to find the vulnerabilities quickly. Many times, some of the vulnerabilities found during the automated scanning are false-positives. These are all eliminated during this phase by manual testing of all the findings.

SSL scan of the various services using SSL is also specifically done during this phase as this is the main line of defense against **Man in the Middle** attacks. There are certain tools available for this specific purpose which can specify if a vulnerable version of SSL is being used and if any weak ciphers are being used for encryption purposes.

TOOLS WE GENERALLY USE IN THIS PHASE:

- Burp suite Pro
- Custom Fuzzers
- Testssl
- ZAP
- Metasploit

PHASE IV - “EXPLOITING THE VULNERABILITIES"

WHAT THIS PHASE IS ABOUT?

It becomes sometimes very important to demonstrate how an attacker can exploit the vulnerabilities found through automated and manual testing. If we have found a vulnerability, then we demonstrate how the attacker in real life can try different methods to exploit the vulnerability. This phase is basically about exploiting these vulnerabilities and see how far they can take us inside the application/network. We develop shells, exploits, codes to demonstrate the exploitability of all the discovered issues.

How ENCIPHERS perform this?

After successful vulnerability detection by automated and manual testing, the team attempts to elevate privileges to gain administrative access to targeted systems and applications and then use the elevated privileges to gain access to sensitive information. More specifically, these are the objectives during the phase:

- To gain unauthorized access to high value information via data stores such as FTP Servers, file shares and databases.
- To gain unauthorized access to systems that could grant further access to the system such as badging, surveillance, jump hosts and account management. Different exploit tools are used in this phase. For a specific vulnerability, there is already a lot of exploitation techniques.

TOOLS WE GENERALLY USE IN THIS PHASE:

- Metasploit
- Privilege escalation exploits
- Sqlmap
- W3af
- BeEF framework
- Enciphers custom tools and scripts

All the tools mentioned in the 4 phases are used in almost all of the penetration tests. But depending upon the type of application, the list of tools can increase so that we do not miss out on even a single hidden/insecure point.

REPORTING

We at ENCIPHERS know the importance of a good report for a penetration test. These are all the things which you will get in the Final Report.

- Hand-written report which will have all the findings shown priority wise from the high priority ones to the low-levels and informative.
- Suggestions for fixing of particular vulnerability will be given in the report for each vulnerability.
- Automated scan reports of Burp Suite Pro, SSL Scan and NMAP scan of the defined target will also be attached with the report, in case these are required.
- All the exploit codes and scripts will be provided as a part of the exploitation description.
- Step by step explanation of vulnerability exploitation, so that it can be reproduced at the client's side too.
- All Proof of concepts (POC) to be provided as a part of the report.