

PENETRATION TESTING REPORT DEMO

|  |  |
| --- | --- |
| REVIEWED BY: Gabriel Marcus | |
| APPROVED BY: | |
| VERSION: 1.0 | DATE:  Valid Until: |

**Table of contents**

[1. Purpose 2](#_Toc491509074)

[2. Project Details / Scope 2](#_Toc491509076)

[3 Reference documents 3](#_Toc491509078)-5

[4. Findings 6](#_Toc491509079)-7

[5. Tools used](#_Toc491509080) 7-8

[6. Snapshots 9-11](#_Toc491509080)

[7. Domain Topology](#_Toc491509080) 12

**8**. **Appendix…………………………………………………………………………………………………………………………. 13**

Purpose:

Security Review for Tiroflx.com Domain and System Computer Infrastructure

Project Details / Scope

Blackbox attack simulation, attack vector inside the network

* Reconnaissance
* Password hashing
* DC LLMNR Exploit
* Operation System Exploits

Whitebox attack simulation, attack vector outside the network

* DNS Enumeration
* Firewall settings test
* DDOS possibility attack

Reference Documents

The Official OWASP Top 10 Vulnerabilities List

**A1. Injection**- Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

**A2. Broken Authentication** - Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

**A3. Sensitive Data Exposure** - Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

**A4. XML External Entities (XXE)** - Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

**A5.Broken Access Controls** - Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

**A6. Security Misconfiguration** - Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

**A7.Cross Site Scripting (XXS)** - XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which

can hijack user sessions, deface web sites, or redirect the user to malicious sites.

**A8. Insecure Deserialization**- Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

**A9. Using Components with Known Vulnerabilities** - Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

**A10. Insufficient Logging & Monitoring** - Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Findings – Black Box Attack

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Findings | Description | Details | Severity | Recommendations |
| Scanned and found DC on same subnet as other Hosts | Used nmap to scan network and found without any issues the DC01 – ADDS Server | <https://www.cvedetails.com/microsoft-bulletin/ms11-030/> | HIGH | **Seperate DC from network , use VLAN's to secure , smb share access as well , IDS should also monitor traffic on DC.** |
| Exploit with Auxilary and Attacked LLMNR packets | Unsecured traffic between DNS and WS allowed for MITM attack to spoof and extract LLMNR hashes = NTLM | <https://www.cvedetails.com/bugtraq-bid/40733/WebKit-NTLM-Credentials-Information-Disclosure-Vulnerability.html> | HIGH | **Need to secure DNS authentication , also setup DNS forwarder to avoid LLMNR Spoofing attacks** |
| No DNS cache Removal or Scavanging configured – arp-a command works on all terminals | Computers remember old hostnames | <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16220> | HIGH | **DNS cache poisoning is a real threat , need to setup scavanging option inside the DNS servers**  **Guide:** <https://www.dell.com/support/article/il/en/ildhs1/sln290798/windows-server-how-to-configure-dns-aging-and-scavenging?lang=en> |
| Psexec tool exploit performed | NTLM Weak hash was cracked with John software , and payload was accessed via exploit with psexec | <https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-4553/Microsoft-Psexec.html> | HIGH | **Stronger password are required to make it harder for bruteforce attacks to be performed.** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Findings – White Box Attack

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dig DNS Extract found Main DNS | Dig Tool used and Zone Transfer was performed | <https://securitytrails.com/blog/8-tips-to-prevent-dns-attacks>  <https://www.cvedetails.com/cve/CVE-1999-0532/> | HIGH | Zone Transfers must be always secured and Audit all trafic in and out of your DNS servers and forwarders via Firewall or Router |

Tools Used:

* NMAP for Windows
* Cain and Abel for Windows
* DNSEnum and NSLookup
* NMAP Power Scripts
* Kali LINUX FOR Whitebox attack
* Pingpath
* Maltego for reconnaissance kill chain attack
* John the ripper for hashing brute force
* PS Exec tools
* Whoami tools
* Web scanners and Burp suite proxy
* The Harverster
* DIG DNS Scanner
* Fierce scanner

### **A scan to search for DDOS reflection UDP services**

|  |  |
| --- | --- |
| Scan for UDP DDOS reflectors | nmap –sU –A –PN –n –pU:19,53,123,161 –script=ntp-monlist,dns-recursion,snmp-sysdescr 192.168.0.0/24 |

### **HTTP Service Information**

|  |  |
| --- | --- |
| Gather page titles from HTTP services | nmap --script=http-title 192.168.0.0/24 |
| Get HTTP headers of web services | nmap --script=http-headers 192.168.0.0/24 |
| Find web apps from known paths | nmap --script=http-enum 192.168.0.0/24 |

### **Detect Heartbleed SSL Vulnerability**

|  |  |
| --- | --- |
| Heartbleed Testing | nmap -sV -p 443 --script=ssl-heartbleed 192.168.0.0/24 |

Heartbleed detection is one of the available SSL scripts. It will detect the presence of the well known Heartbleed vulnerability in SSL services. Specify alternative ports to test SSL on mail and other protocols

### **IP Address information**

|  |  |
| --- | --- |
| Find Information about IP address | nmap --script=asn-query,whois,ip-geolocation-maxmind 192.168.0.0/24 |

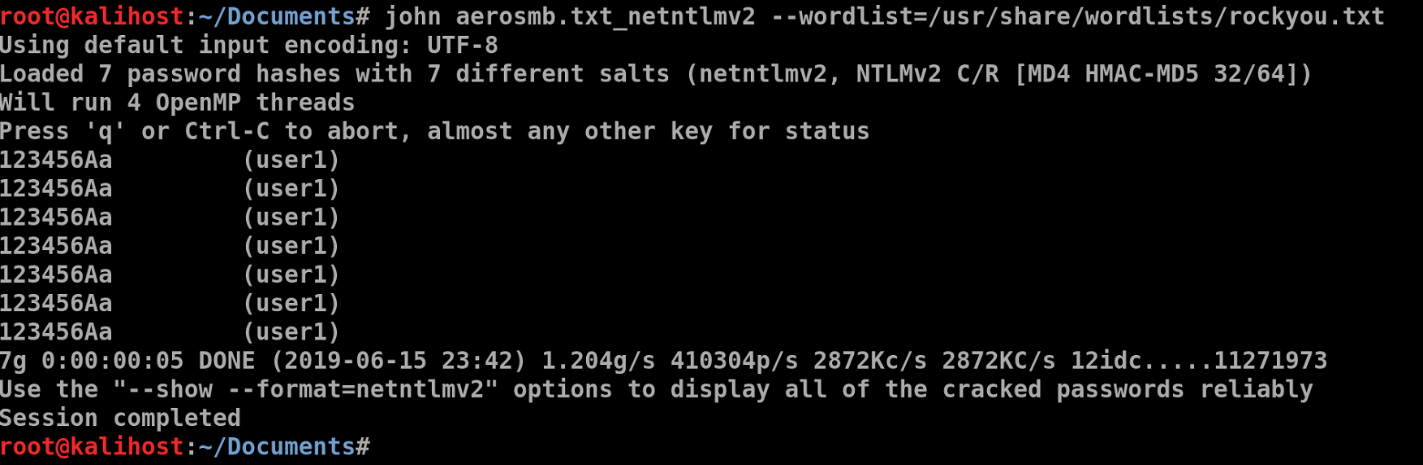
Gather information related to the IP address and netblock owner of the IP address. Uses ASN, whois and geoip location lookups.

SNAPSHOTS

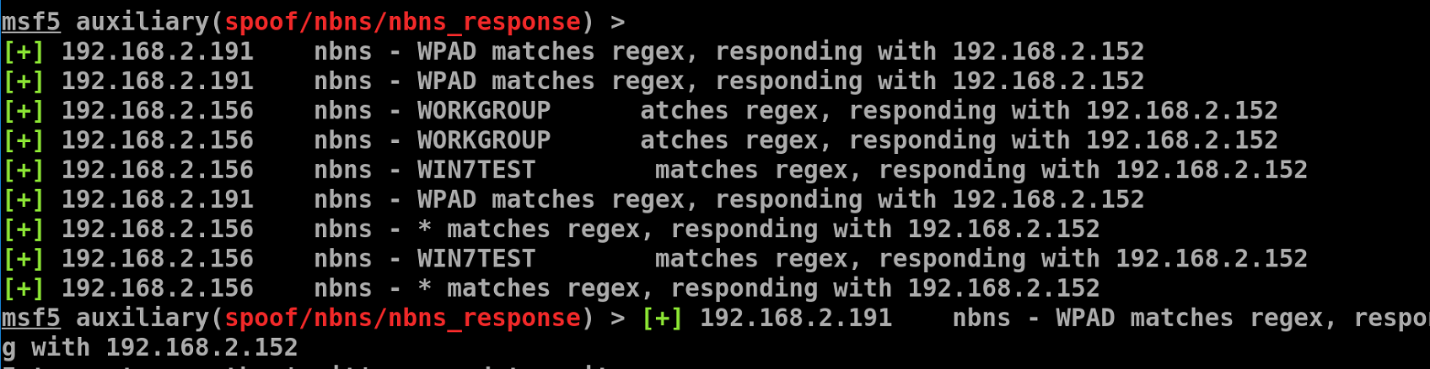
DNS Zone Transfer



NTLM Hash Brute force crack



NBNS Responds



LLMNR Responds

