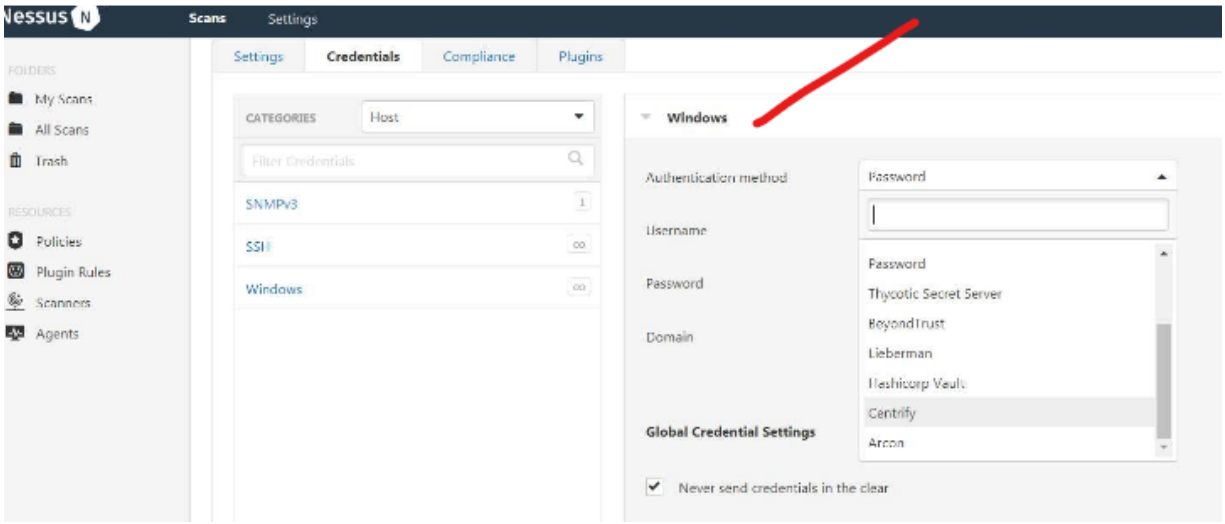
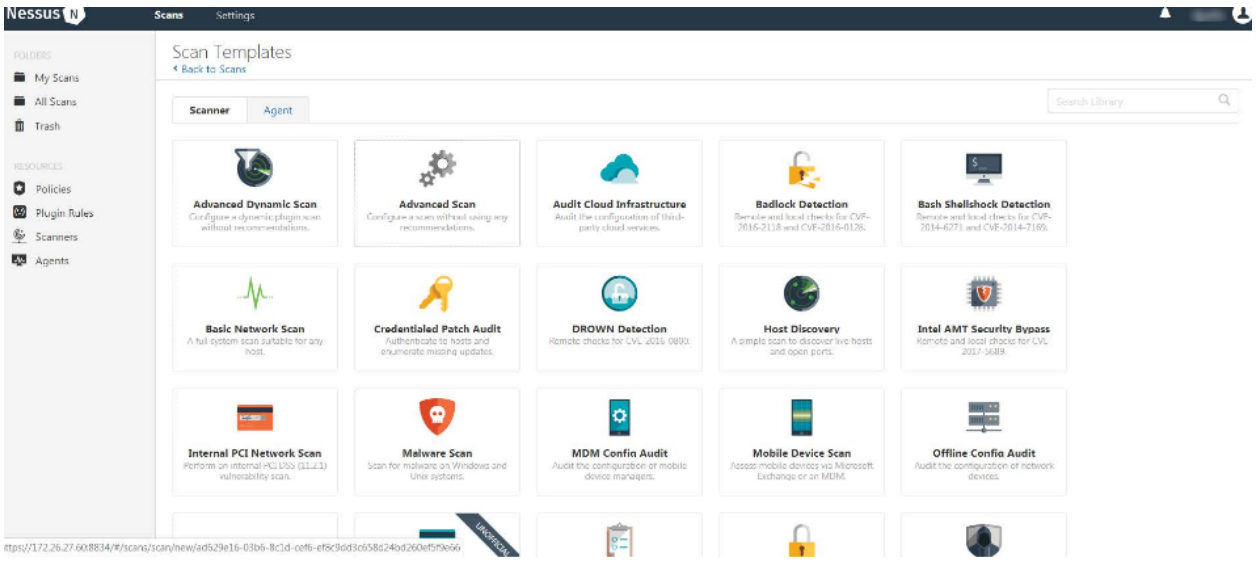
Phase 3: Identify Vulnerabilities

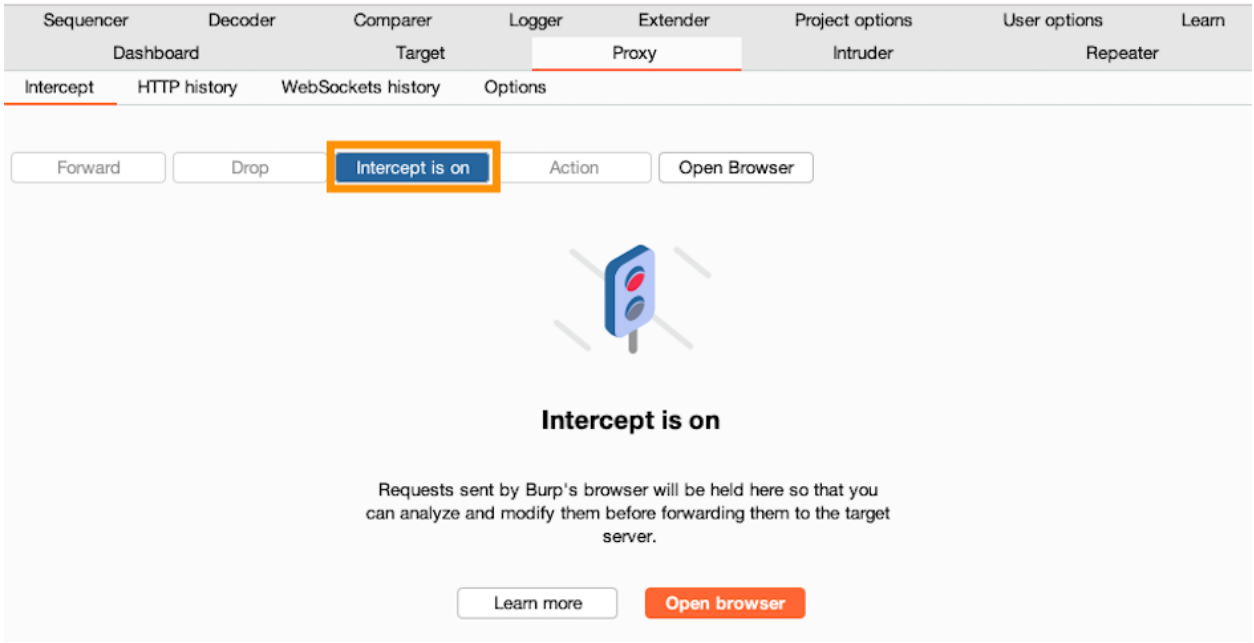
We will use our vulnerability scanners to inspect the target's computers and network for potential weakness.Our vulnerability scan will detect weakness in all the targets communication equipment and give us a prediction of countermeasures .Our systems are designed to check for live systems ,live host, operating systems,architecture of target systems. and to check for open ports .Once discovery is completed we will implement malicious attacks though all found attack vectors .Once attack vectors are detected we will enumerate all data on the target's entire network including end-user devices .

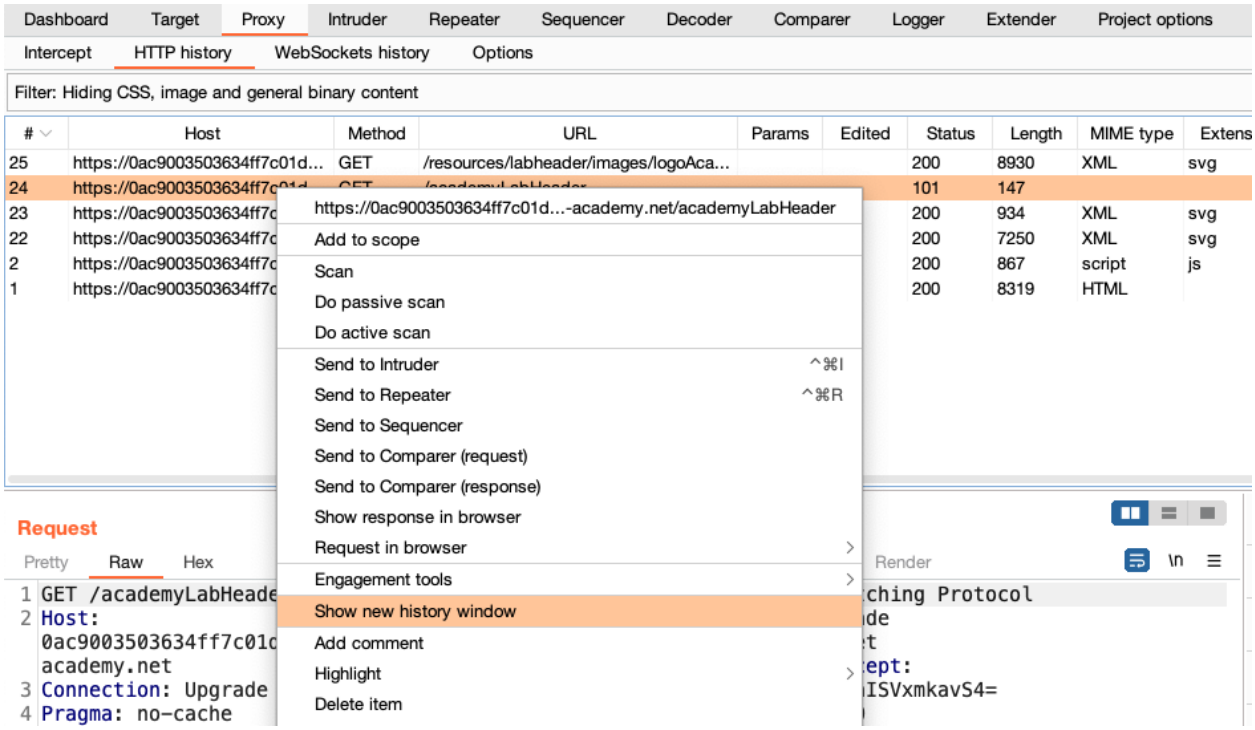
The first tool we will use is the Nessus vulnerability scanner. It is an open source remote scanning tool that scans computers for vulnerabilities that we will use to enumerate data from our target. Nessus has many features but we will use it for its high-spend speed asset discovery and sensitive data discovery .Nessus has the ability to identify if compliance requirements are met on different host on the target network however this not a key feature Nessus also bring bad news to our mission with its slowness when scanning a large targets such are target we will also suffer when we chose to scan deep Nessus will consume more resources


Nessus
Scans
Settings
Settings
Credentials
Compliance
Plugins
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Agents
CATEGORIES
Host
Filter Credentials
SNMPv3
SSH
Windows
Windows
Authentication method
Password
Username
Password
Domain
Global Credential Settings
Password
Thycotic Secret Server
BeyondTrust
Lieberman
Hashicorp Vault
Centrify
Arcon
Never send credentials in the clear

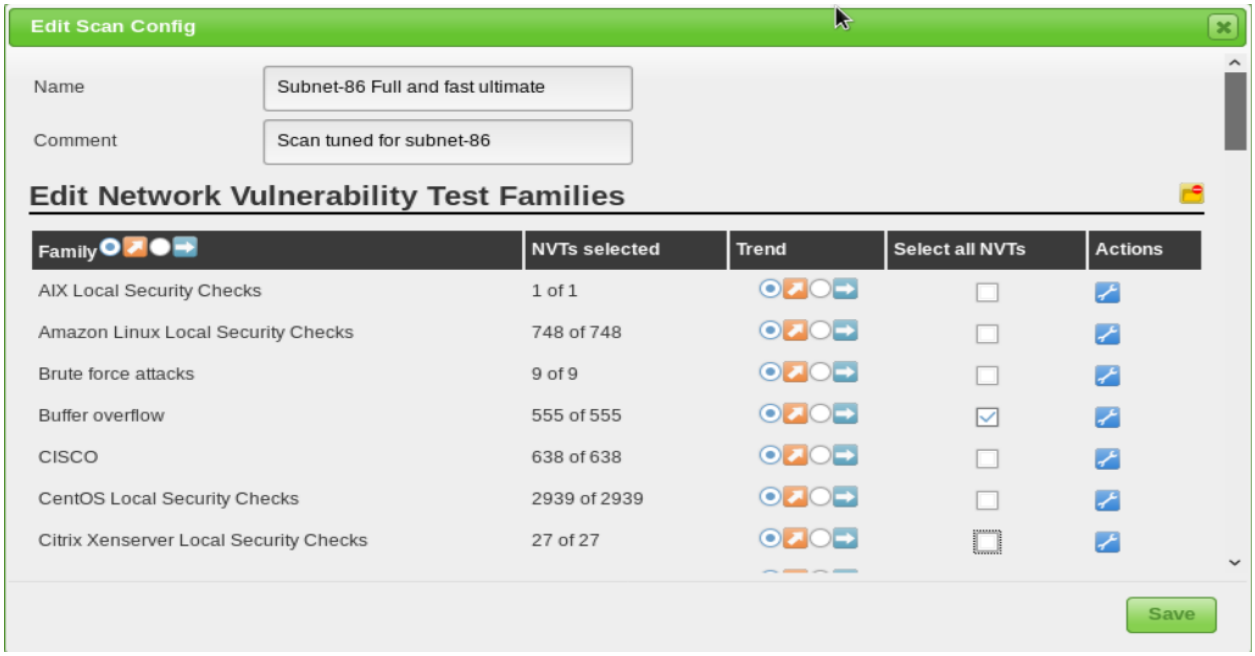

Nessus
Scans
Settings
Scan Templates
Back to Scans
My Scans
All Scans
Trash
Policies
Plugin Rules
Scanners
Agents
Scanner
Agent
Search Library
Advanced Dynamic Scan
Advanced Scan
Audit Cloud Infrastructure
Badlock Detection
Bash Shellshock Detection
Basic Network Scan
Credentialed Patch Audit
DROWN Detection
Host Discovery
Intel AMT Security Bypass
Internal PCI Network Scan
Malware Scan
MDM Config Audit
Mobile Device Scan
Offline Config Audit

Burp Suite is a widely used web app penetration testing tool .It is a integrated platform tool with a graphical user interface that performs security testing of the targets web application .We will use Burp Suite to exploit the targets web applications and gain access to confidential data .We will also take advantage of Burp Suite ability to intercept request messages,Burp Suite can perform automated and manual testing performing both task in one tool .Burp Suite interface can bring problems as well and is merely designed for applications/browsers and doesn't cover other types of traffic.





Now that we have a tool that will discover and incept web applications request , we will implement OpenVas to handle other parts of our penetration test .OpenVas is a vulnerabilities scanner that is considered a full feature and allows for unauthenticated and authenticated testing .We will focus on Open\vas ability to discover know vulnerability such as cross site scripting and improper file access we will use to enumerate data .One of the pros of using OpenVas is that it provides a feature that allows us to configure the product to our own requirements if needed .On the flip side OpenVas covers less vulnerabilities and has limited operating system support .



Vulnerability	Severity	QoD	Host	Location	Actions
X Server	10.0 (High)	80%	192.168.56.101	6000/tcp	
PostgreSQL weak password	9.0 (High)	99%	192.168.56.101	5432/tcp	
PostgreSQL Multiple Security Vulnerabilities	8.5 (High)	80%	192.168.56.101	5432/tcp	
TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80%	192.168.56.101	80/tcp	
phpinfo() output accessible	7.5 (High)	80%	192.168.56.101	80/tcp	
ProFTPD Long Command Handling Security Vulnerability	6.8 (Medium)	80%	192.168.56.101	2121/tcp	
PostgreSQL Multiple Security Vulnerabilities	6.8 (Medium)	80%	192.168.56.101	5432/tcp	
phpMyAdmin Bookmark Security Bypass Vulnerability	6.5 (Medium)	80%	192.168.56.101	80/tcp	
PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability	6.5 (Medium)	80%	192.168.56.101	5432/tcp	
PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability	6.5 (Medium)	80%	192.168.56.101	5432/tcp	
PostgreSQL PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability	6.0 (Medium)	80%	192.168.56.101	5432/tcp	
http TRACE XSS attack	5.8 (Medium)	99%	192.168.56.101	80/tcp	
PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability	5.5 (Medium)	80%	192.168.56.101	5432/tcp	
Check if Mailserver answer to VRFY and EXPN requests	5.0 (Medium)	99%	192.168.56.101	25/tcp	
/doc directory browsable ?	5.0 (Medium)	80%	192.168.56.101	80/tcp	
TikiWiki CMS/Groupware Input Sanitation Weakness Vulnerability	5.0 (Medium)	80%	192.168.56.101	80/tcp	
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	192.168.56.101	22/tcp	

Metasploit is a powerful vulnerability tool that is widely used by ethical hackers.We will use Metasploit to probe the target's system for vulnerabilities on their servers. Metasploit can easily be customized and is compatible with most operating systems . We use Metasploit for its ability to penetrate servers .Metasploit uses automated testing to exploit a vulnerability the ease of switching between payloads allows quick access .Metasploit is not all good news the limited graphical user interfaces can be a problem and if not handled properly the system can crash .

Our last tool is Acunetix. It is a vulnerability scanner that allows us to use speed and fast scanning .Vulnerabilities will be revealed in an instant of being found. We use Acunetix for its ability to get to hard to find places such as password protected areas ,unlinked pages and script heavy sites built with javascript .Acuneix has many excellent features such as being able to recognize vulnerabilities and false positives .The cons of Acunetix revolve are no support on multiple endpoints and problems with authentications.These tools will provide the necessary outputs that will allow us to be successful with our attempt to exploit our target .