Phase 2: Identify Targets and Run Scans

Now we will discuss and explain identifying the targets and scanning tools we will use and employ in detail .We will review the tools and techniques to be used to perform host discovery and enumeration .The discuss the description and purpose of each tool and the challenges and potential drawbacks or limitations they may have .Scanning tools can find vital information and aid in a successful hack .We will need to used all of the technology correctly in order for us to find vulnerability properly .The tools we will utilize will be Nessus,OpenVas and Burp Suite all of these tools are open source software provide vulnerability scanning with unique features.

Nessus provides remote security scanning that raises an alert if it discovers vulnerabilities .Nessus passive network scanning puts emphasis on monitoring network activity which is what we need for this penetration test .The biggest drawback or limitation with Nessus is that the software can be difficult to use and it doesn't always scan with the credentials needed to have a proper scan.Another drawback with Nessus is it is not accurate in certain situations .This could be detrimental to our efforts towards a successful exploit. OpenVas will serve as a full-feature vulnerability scanner that has the capability to perform un-authenticated and authenticated testing .We will use OpenVas for its internal programming language which will allow us to implement various types of vulnerability testing .

The limitations we might experience with OpenVas is that it has less operating system support ability this could limit us to certain resources .Nmap is a network scanning tool that at its core uses IP packets to identify devices that attached to the network .Nmap also provides information on operating systems that we will take advantage of once we can exploit the targets network,application and end-user hosts . We will use Nmap by executing banner grabbing techniques to get intel on the target .Nmap is a

great tool however,it has drawbacks that could interfere with attempts to exploit vulnerabilities .Nmap can be blocked by Antivirus software which may affect depth and accuracy of data of scans .

Metasploit framework allows us to quickly search a targeted IP range and find vulnerabilities and find weak points in our targets network .Metasploit scan will give us a indication of which attack surfaces are worth exploiting .The drawbacks and limitation of Metasploit can include the risk of our systems crashing and difficulty of use if we run the program on a host that have Antivirus software .Wireshark is a multi-platform network protocol analyzer .It will allow use to see the targets network on a microscopic level .Wire will also allow us to read or write different capture file formats particularly tcpdump and Pcap NG.Although wireshark is the a widely used network analyzer their are limitations that could hinder our progress such as wireshare being limited to only gathering information from the network and not being able to send that information .These are the network scanning tools we will use to infiltrate our target .