Hacker Methodology
Hacker Methodology

- Footprinting
- Scanning
- Enumeration
- Network Mapping
- Gaining Access
- Privilege Escalation
- Post Exploitation
Footprinting: This is the process of conducting target analysis, identification, and discovery; typically through the use of open source tools. This includes dumpster diving, social engineering and the use of utilities such as web-search hacking, traceroutes, pings, network lookups, etc.
**Scanning**: This step will take the findings from footprinting and begin to drill-down a bit further. In a traditional sense, this step includes port scanning, OS identification, and determining whether or not a machine is accessible.
**Enumeration:** This is the phase where you further interrogate specific services to determine exact operating systems, software, etc. Normal enumeration techniques include searching for network share information, specific version of applications running, user accounts, SNMP traffic, etc.
Network Mapping: This step is exactly as the name implies, laying out an illustration of the targeted network. This includes taking all available resources (logs, target surveys, etc) to create a visualization of the target environment. This often looks different from the exploiters perspective then from the Admin’s perspective. Depending on the scope of activities being conducted this step may or may not be necessary.
Gaining Access: This step is the exploitation process. Basically, this is gaining access to the machine or the network by a client-side exploit, insider threat, supply interdiction attack, or remote exploitation opportunity. This could be conducted via spear-fishing attacks, buffer overflows, embedded device exploitation, credential masquerade attacks, etc.
Privilege Escalation: Depending on the exploitation opportunity which was used the attacker may need to elevate privileges to a different user. There are various different scenarios in which the attacker will need to use this procedure. Typically, this is conducted through the use of a local exploit opportunity in order to gain root or system-level privileges – the highest possible user.
Post Exploitation: This step is really a compilation of many steps and is dependent upon the objective of the mission. This step could include any combination or all of the following examples:

- Target Survey & Remote Forensics Analysis
- Cover Tracks (cleanup)
- Data Collection
- Rootkit (aka Backdoor, Implant, Persistence)
- Computer Network Attack
  - Disrupt
  - Deny
  - Degrade
  - Deceive
  - Destroy
  - Delay
**Target Survey & Remote Forensics Analysis:** This step is to conduct analysis on the target machine for potential security mechanisms, files, or users which could either assist in obtaining the objective or harm the assessment. This is the process of analysing the targets operating environment.
Cover Tracks (cleanup): This step is the process of removing any forensically relevant residue that was left behind as the result of exploitation or presence. This is one of the most important steps that a hacker can perform to maintain stealth. This is often one of the most important opportunities for defenders to profile an attacker.
**Data Collection**: The attacker is in the network to perform some activity. Usually, this is not to show Cyber prowess, but instead to extract as much data as possible. Network traffic analysis is key during this phase.
Rootkit (aka Backdoor, aka Implant, aka Persistence): This step is the process of installing an application, hooking the kernel, or laying down some mechanism which allows the attacker to maintain continued access to the host or network. If the implant is well designed, the attacker can live in your network for extended periods of time.
**Computer Network Attack.** In this step the attacker has already identified the network as a target of opportunity and has identified plans to launch an attack. This attack could be remote or local in nature and could come from already established access or with no access to the targeted environment. The attacker will typically identify core and vital network processes and perform various attacks to disrupt, deny, degrade, destroy, or deceive their “adversary.”

The most sophisticated attackers would likely obtain access to the target environment. After obtaining access to the critical infrastructure, techniques will be utilized to achieve the 5D’s of Computer Network Attack.
Exploitation Preparation. Before beginning an exploit the attacker needs to prepare his environment, this starts with selection of an exploitation platform. But which should I choose?

Kali Linux (previously BackTrack)

- Open Source (Free) Platform
- Debian-based Distribution
- Over 300+ Penetration Tools
- Incorporates Forensics Capabilities
- Supports ARM Architecture
Username: root
Password: toor
NMAP – Network Mapper

✓ Generates Network Traffic to Specific Hosts or Range of Hosts
✓ Determines Open\Closed Network Ports
✓ Supports multiple protocols
✓ Can identify Operating System
✓ Helps identify potential vulnerable services
✓ Fast and Stable – sacrifices some stealth
root@kali:~# nmap -sP 172.16.78.0/24

Starting Nmap 6.25 ( http://nmap.org ) at 2014-01-05 13:45 CST
Nmap scan report for 172.16.78.0
Host is up (0.000s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 172.16.78.2
Host is up (0.000s latency).
MAC Address: 00:50:56:F0:28:DB (VMware)
Nmap scan report for 172.16.78.131
Host is up (0.0018s latency).
MAC Address: 00:0C:29:C2:F0:02 (VMware)
Nmap scan report for 172.16.78.151
Host is up.
Nmap scan report for 172.16.78.254
Host is up (0.00001s latency).
MAC Address: 00:50:56:FA:C9:08 (VMware)
Nmap done: 256 IP addresses (5 hosts up) scanned in 4.60 seconds
root@kali:~#
root@kali:~ # nmap -ss 172.16.78.131 -p 21,22,23,80,135,139,443,445

Starting Nmap 6.25 ( http://nmap.org ) at 2014-01-05 13:44 CST
Nmap scan report for 172.16.78.131
Host is up (0.0012s latency).
PORT     STATE    SERVICE
21/tcp   closed  ftp
22/tcp   closed  ssh
23/tcp   closed  telnet
80/tcp   closed  http
135/tcp  open    msrpc
139/tcp  open    netbios-ssn
443/tcp  closed  https
445/tcp  open    microsoft-ds
MAC Address: 00:0C:29:C2:F0:02 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
root@kali:~ #
Metasploit Framework

- Security Vulnerability Framework
- Excellent vulnerability identification
- Programmed mostly in Ruby
- Supports many operating systems
- Already installed on Kali
- Free
- Customizable
Exploit Database

Website For Security Engineers to Upload Discovered Vulnerabilities

- Google Hacking Strings
- Remote Exploits
- Local Exploits
- Denial of Service
- Shellcode
- Research Papers
Questions