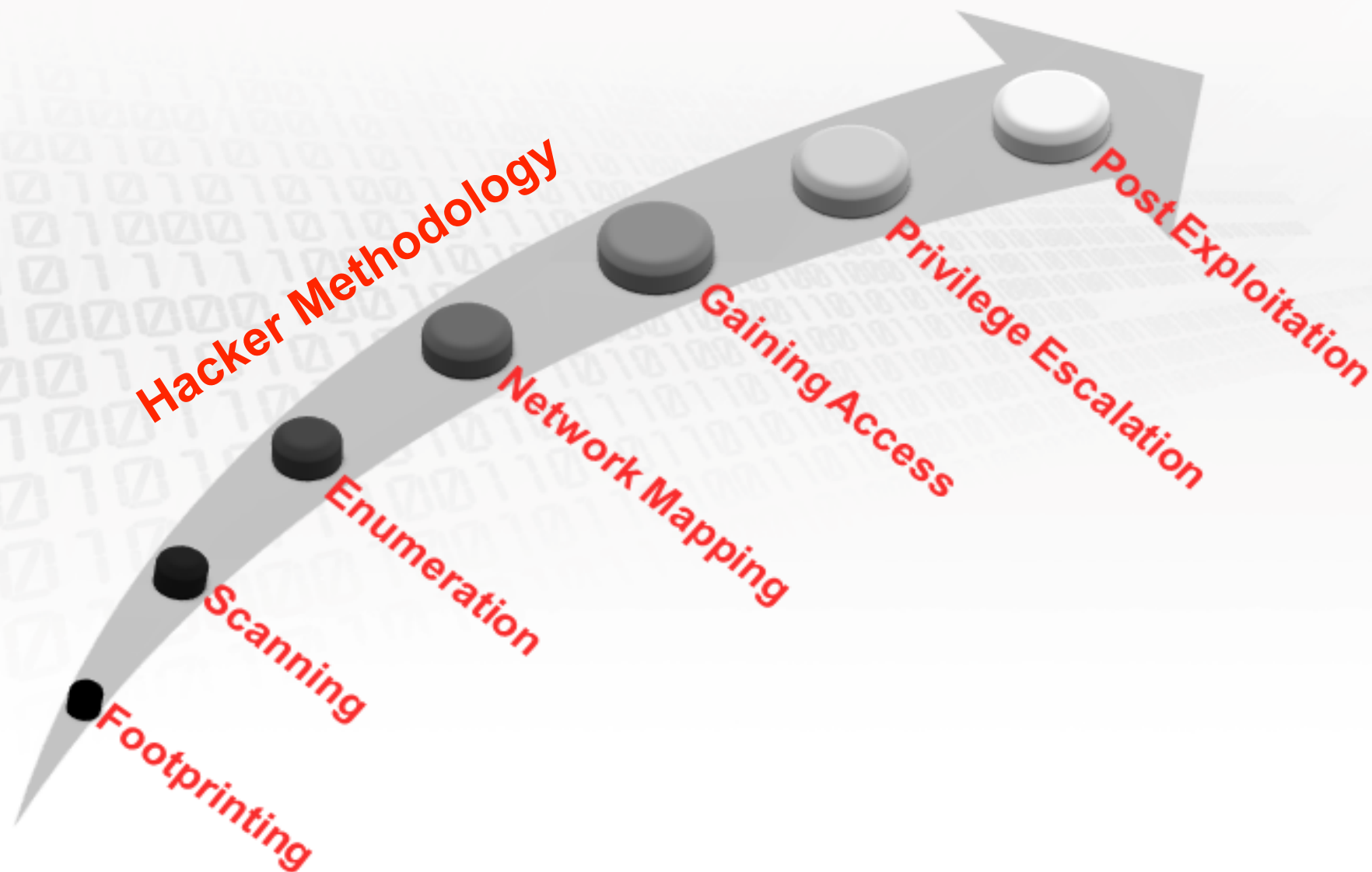


Hacker Methodology



Hacker Methodology



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.

Platform Selection

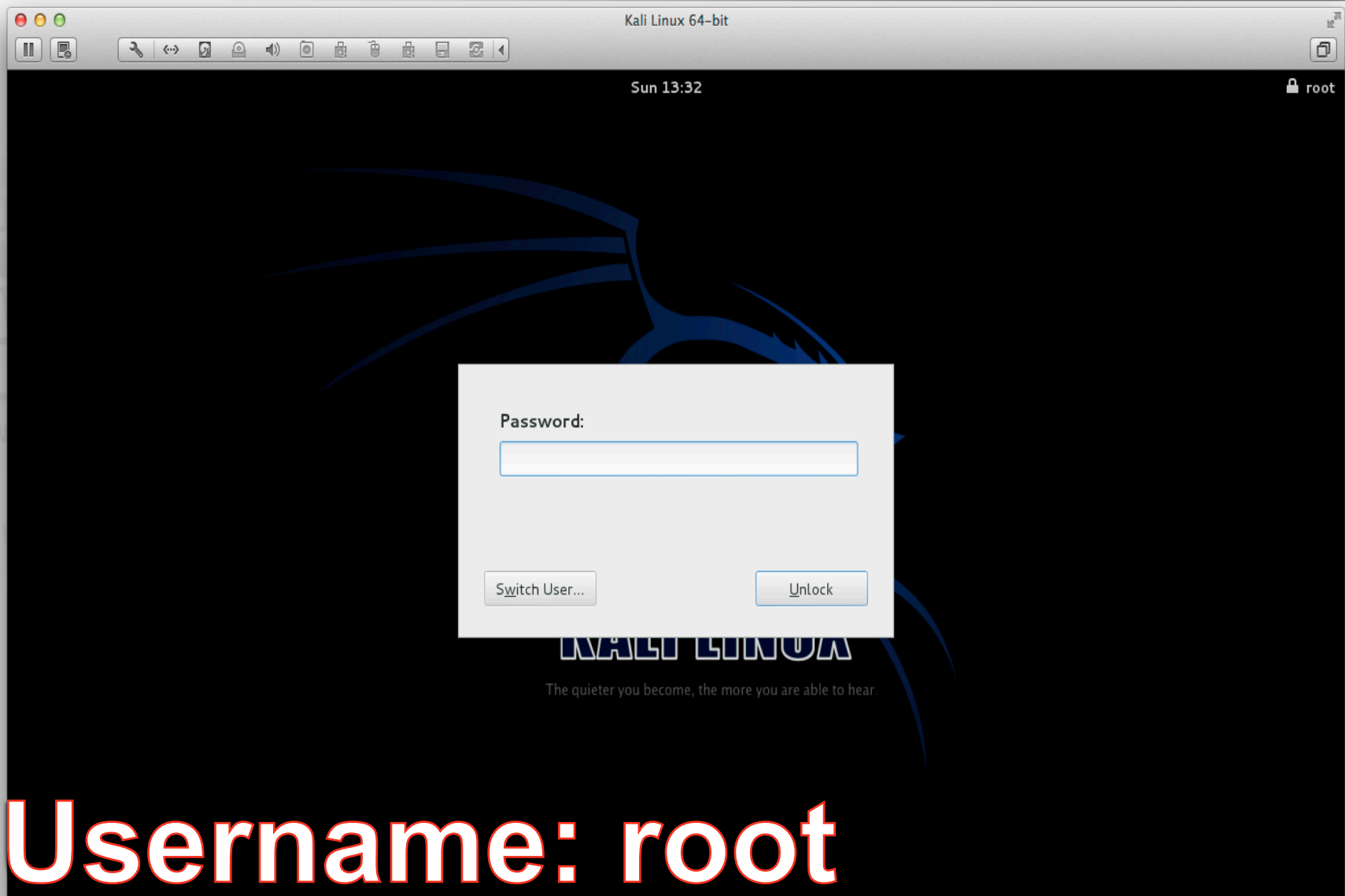


Exploitation Preparation. Before beginning an exploit the attacker needs to prepare his environment, this starts with selection of an exploitation platform. But which should I choose?

Kali Linux (previously BackTrack)

- ✓ Open Source (Free) Platform
- ✓ Debian-based Distribution
- ✓ Over 300+ Penetration Tools
- ✓ Incorporates Forensics Capabilities
- ✓ Supports ARM Architecture



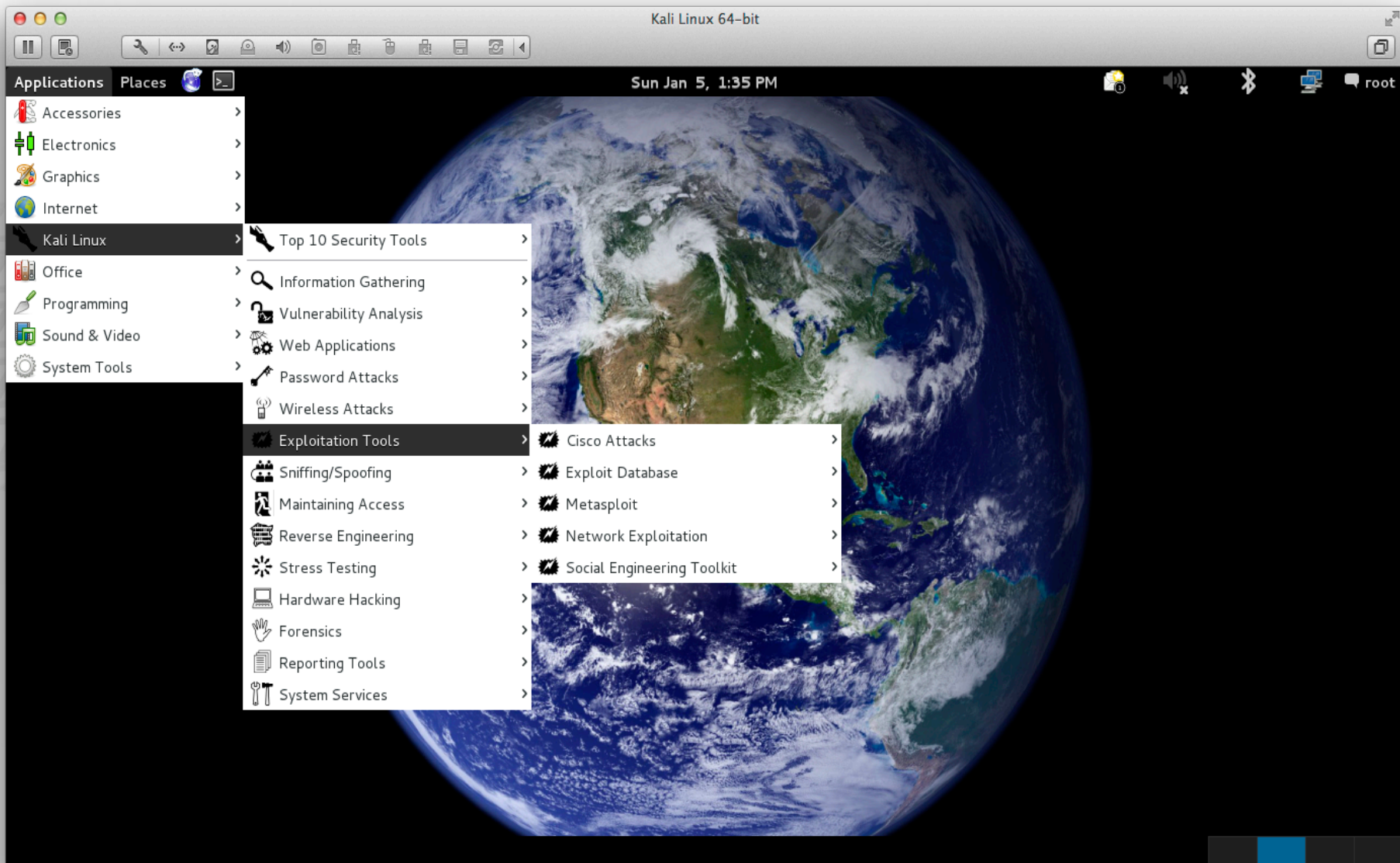


Username: root

Password: toor

root9B



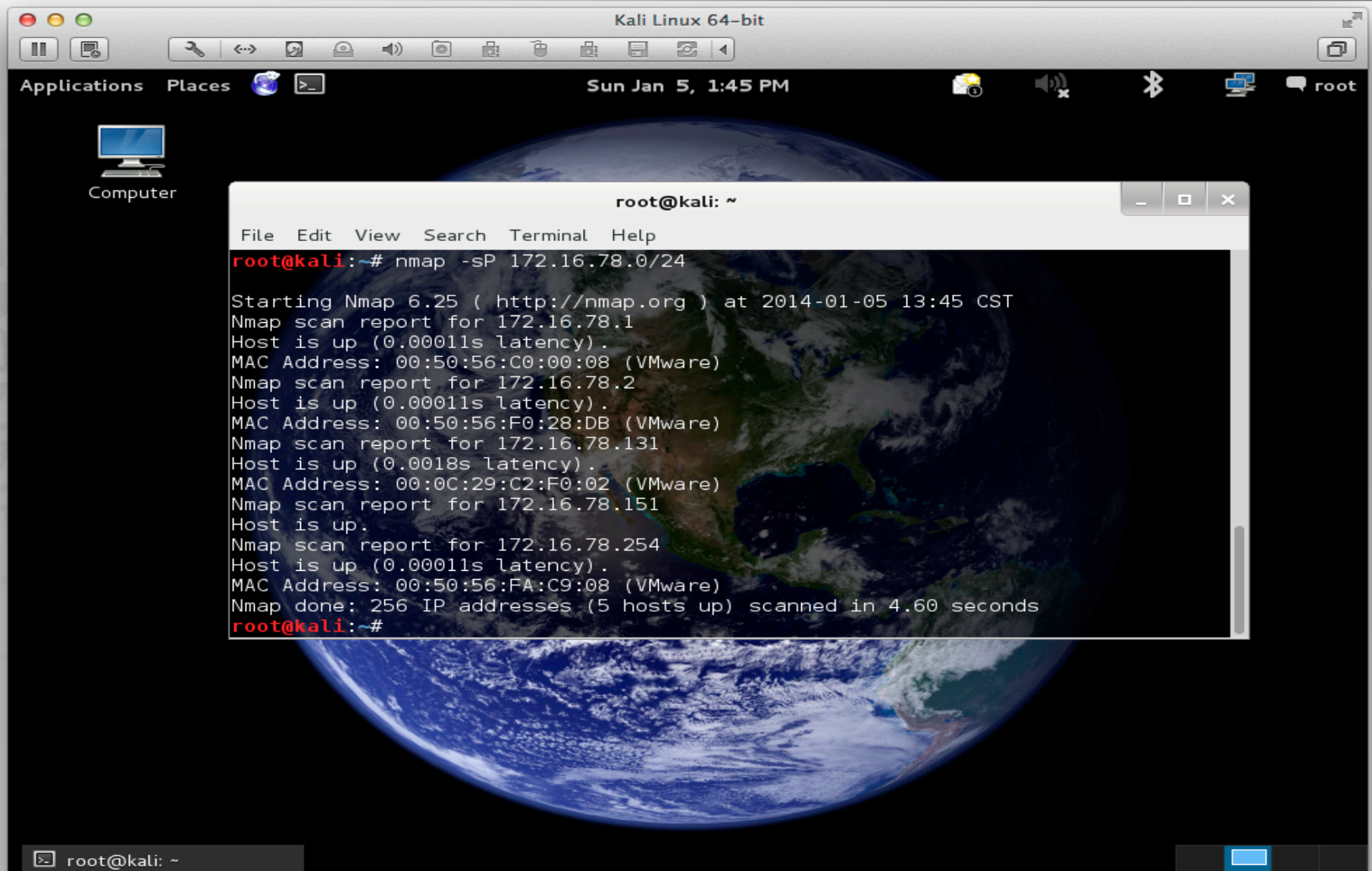


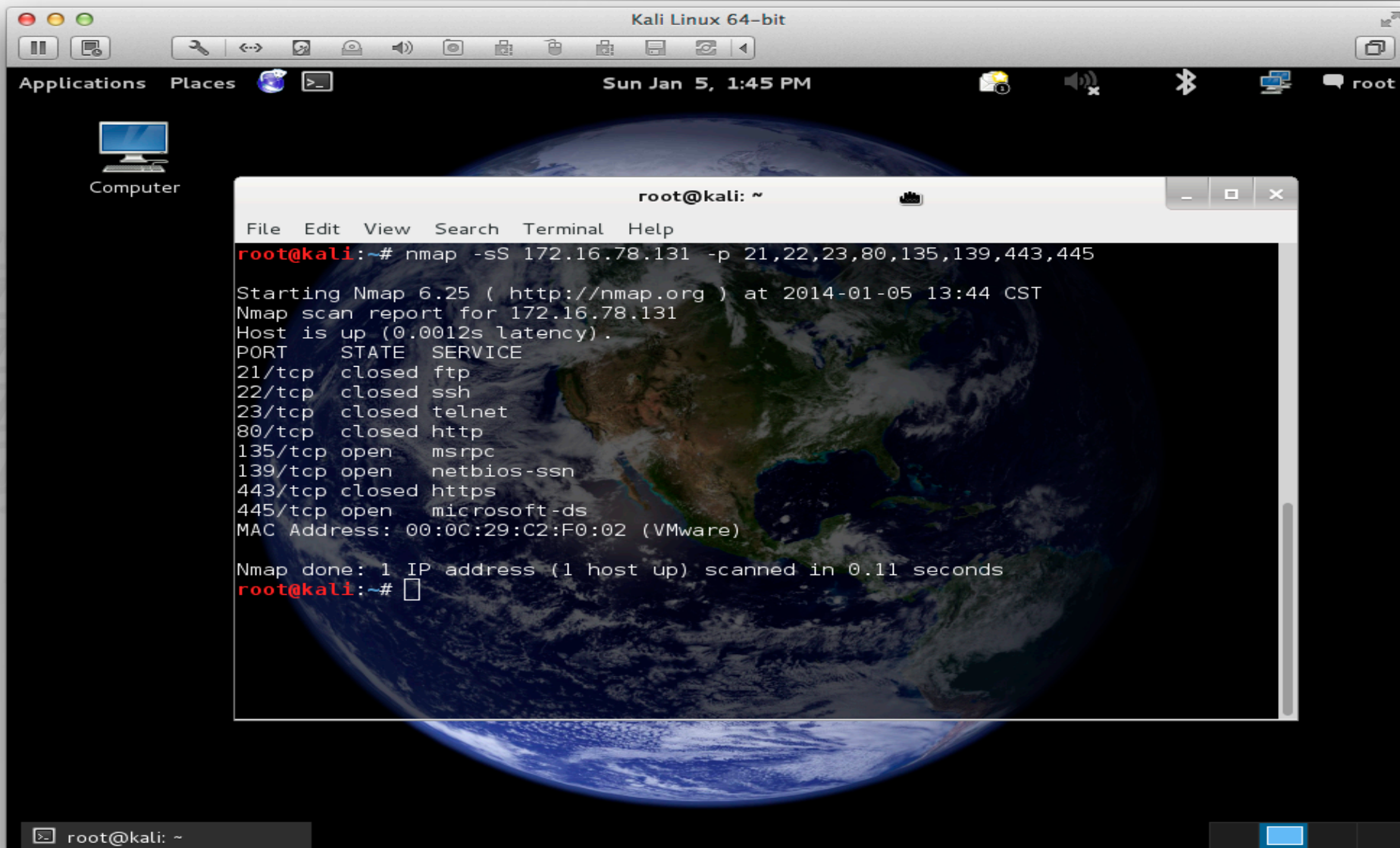
Scanning



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



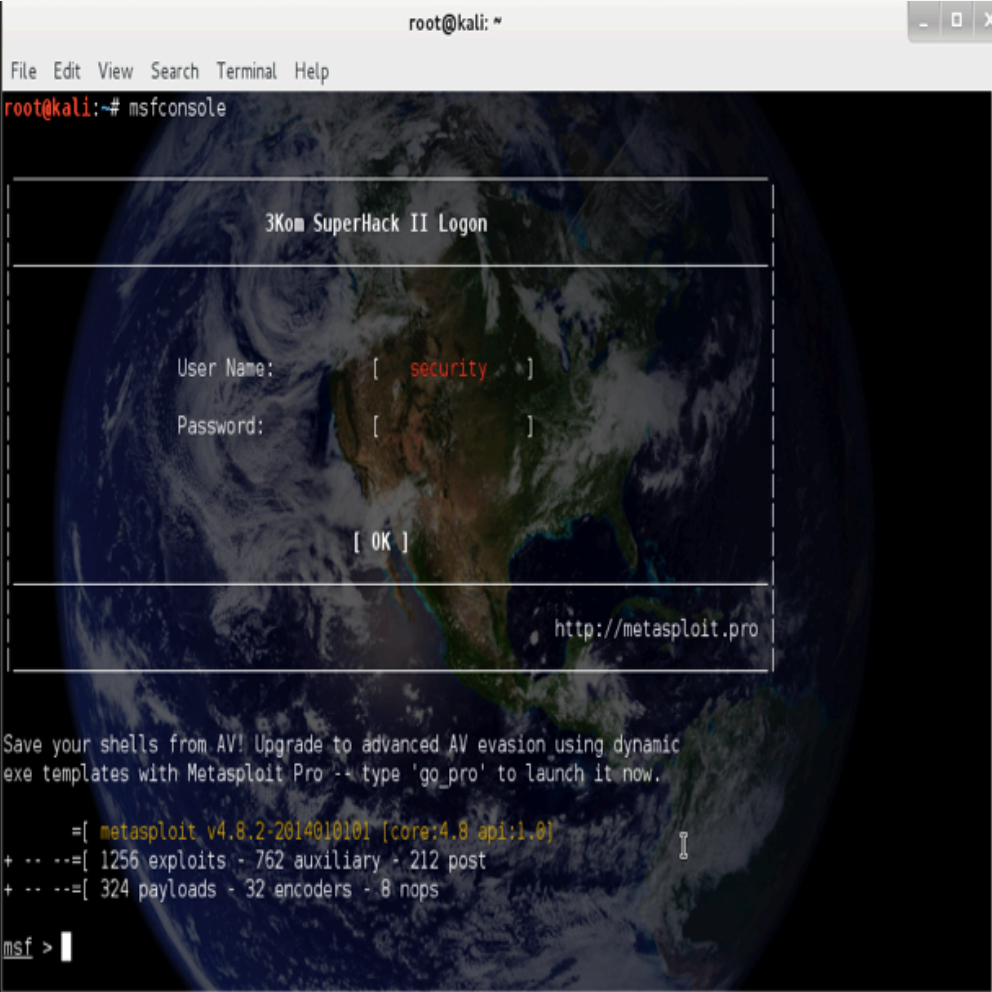


Exploitation



Metasploit Framework

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



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole

3Kom SuperHack II Logon

User Name: [ security ]
Password: [ ]

[ OK ]

http://metasploit.pro

Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

=[ metasploit v4.8.2-2614010101 [core:4.8 api:1.0]
+ -- ==[ 1256 exploits - 762 auxiliary - 212 post
+ -- ==[ 324 payloads - 32 encoders - 8 nops

msf >
```


Exploit Database

Website For Security Engineers to Upload Discovered Vulnerabilities

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

The screenshot shows the Exploit Database website. The header features the 'EXPLOIT DATABASE' logo, social media links for blog, exploit, and Facebook, and a status bar indicating 'Currently Archiving 27084 Exploits' and 'Updated (CVE And Archive): Sun Jan 5 2014'. A navigation bar includes links for HOME, GHDB, ABOUT, REMOTE, LOCAL, WEB, DOS, SHELLCODE, PAPERS, SEARCH, and SUBMIT. Below the navigation bar is a banner for 'OFFENSIVE security' with the text 'Then register for our online training courses today!'. The main heading is 'The Exploit Database', followed by a description: 'The Exploit Database (EDB) - an ultimate archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database.' Below this is a section titled 'Remote Exploits' containing a table of exploit entries.

Date	D	A	V	Description	Plat.	Author
2013-12-24	↓	-	✓	Red Hat CloudForms Management Engine 5.1 - agent/Unixpkgs Path Traversal	376 linux	metasploit
2013-12-24	↓	-	✓	Synology DiskStation Manager - SLICEUPLOAD Remote Command Execution	216 unix	metasploit
2013-12-24	↓	-	✓	OpenSIS 'modname' - PHP Code Execution	171 linux	metasploit
2013-12-24	↓	-	✓	Zimbra Collaboration Server - LFI	231 linux	metasploit
2013-12-24	↓	-	✓	HP SiteScope IssueSiebelCmd - Remote Code Execution	143 unix	metasploit
2013-12-24	↓	-	✓	Firefox 5.0 - 15.0.1 - __exposedProps__ XCS Code Execution	303 windows	metasploit
2013-12-17	↓	-	✓	Adobe Reader ToolButton - Use After Free	587 windows	metasploit

Questions

