KYRION Technologies

Winter Camp

COURSE CURRICULUM

ADVANCED ETHICAL HACKING

XPLOIT The Next Level

Xploit - Advanced Ethical Hacking Curriculum

Duration

Lecture and Demonstration: 20 Hours

Introduction

Xploit has been specially designed for the students who are really keen to move a step ahead. The module has been carefully drafted by the Core Hackers of Kyrion Digital Securities in synchronization with top securities experts of India and professors of top colleges of India.

It will cover important nuances like Windows Buffer Overflow Exploitation, WPA & WPA2 Cracking, Creating Rouge Access Point, Linux Root Password Cracking, Creating Viruses for Linux Based Systems, Man In The Middle Attacks, DNS Poisoning, Web Application Brute Forcing, and many more such challenging and interesting topics.

Join us to explore the unexplored aspects of Hacking & Exploitation:

- In and Out of Buffer Overflow Exploitation with MetaSploit Framework, Meterpreter, Armitage, Evilgrade, Fast track, etc. Get hold of any PC, just by knowing its IP Address.

- Own the Network like the Administrator. Watch other's chat, kill their downloads, modify network data and get everyone's login details.

- Crack the WPA and WPA-2 Passwords. Create Fake Wireless Access Points and fool the users to get their passwords.

- Control the database server from login panel and run any DB query. Automated SQL Injection along with other fascinating attacks.

- Crack the Linux Root password, create viruses for Linux and make backdoors. Declare that Linux is not too secure.

- Adapt Virtual PCs, safe yourself from your own R&D. Follow the policy "Don't Hack Yourself".

Detailed Module

Buffer Overflow Attacks

In the present competitive world, Programmers have a difficult job. Faced with tight deadlines and the need to get products to market quickly, security might be the last thing on their minds. The first series of tests are probably performed by the programmers and quality engineers to get an idea of how applications will function. Beta testing comes next and might be performed internally and externally by prospective users, but after that it's off to market.

A generic Buffer Overflow occurs when a buffer that has been allocated a specific storage space, has more data copied to it than it can handle.

- Introduction to Buffer, Heap and Stack
- What is Buffer Overflow?
- Exploiting an Overflow in Buffer
- Types of Buffer Overflow Attacks
  - o Heap Based Buffer Overflow
  - o Stack Based Buffer Overflow
- NOPS (No-Operation instructions)

A Buffer Overflow can allow an intruder to load a remote shell or execute a command, allowing the attacker to gain unauthorized access or escalate user privileges. To generate the overflow, the attacker must create a specific data feed to induce the error, as random data will rarely produce the desired effect. These attacks can also be automated using some Pre-configured Tools and Scripts.

- Tools Used in Buffer Overflow Attacks
  - o Meta-Sploit in Windows
  - o Backtrack Meta-Sploit Framework

A Buffer Overflow occurs when data written to a buffer, due to insufficient bounds checking, corrupts data values in memory addresses adjacent to the allocated buffer. Most commonly this occurs when copying strings of characters from one buffer to another. Let us take a close look at some of the most popular applications getting exploited using Buffer Overflow Attack.

- Addons for Metasploit Framework o Fastrack
  o SET
  Tabnabbing

- Other available Frameworks
  - o Evilgrade
  - o Armtage

Now we have learned that how to use existing exploits let us start with writing our own exploits. Perl language can be used for creating scripts and bound checking of the allocated buffer.

- Introduction to Scripting languages

- Basics of Perl
  - o Datatype
  - o Variables
  - o Declaration
  - o Syntax

- Checking boundary of Application's buffer
- Going beyond to boundary of allocated buffer
- Exploiting Application

Various techniques have been used to detect or prevent buffer overflows, with various tradeoffs. The most reliable way to avoid or prevent buffer overflows is to use automatic protection at the language level. This sort of protection, however, cannot be applied to legacy code, and often technical, business, or cultural constraints call for a vulnerable language.

- Protective countermeasures
  - o Choice of programming language
  - o Use of Safe Libraries
  - o Pointer protection

Exploiting Network

Computer networks get a bad rap in the movies. Fear not. These bad networks exist only in the dreams of science-fiction writers. Real-world networks are much more calm and predictable. They don't think for themselves, they can't evolve into something you don't want them to be. As a network administrator, it is important that you understand the nature of potential attacks on computer security.

- Networking Terminologies
- Networking Devices
- Types of Network
- Three Way Handshake

There are a number of reasons why an individual(s) would want to attack corporate networks. The individuals performing network attacks are commonly referred to as network attackers or hackers or crackers. A few ways to compromise a Network would include:

- Network Enumeration
- MAC Spoofing
- Sniffing
- ARP Poisoning - Man in the Middle Attack
- DNS Spoofing
- SSL Strip
- Pharming
- Creating Proxy Server
- Creating logs
- Faking Sites
- Denial of Service Attack

There is a race between the attackers, who try to find loopholes, and the vendors, who develop patches for them. Capable motivated attackers may find exploits for themselves and keep quiet about them, but most reported attacks involve exploits that are not only well known but for which tools are available on the Net

- Tools Used in Network Attack
  - o Ethereal
  - o Ettercap
  - o Wireshark
  - o SSLStrip.

To protect your network infrastructure, you need to be able to predict the types of network threats to which it is vulnerable. This includes an analysis of the risks that each identified network threat imposes on the network infrastructure

- Detecting Network Attacks.

The Internet Protocol Suite (or the Network) was designed for a world in which trusted hosts at universities and research labs cooperated to manage networking in a cooperative way. That world has passed away.

- Securing Network Perimeter
  - o Concept of Firewalls
  - o Intrusion Detection Systems
  - o Configuring Firewall on Windows Operating System

Wireless Network Exploitation

Demand for wireless access to LANs is fueled by the growth of mobile computing devices, such as laptops and personal digital assistants, and by users' desire for continuous network connections without physically having to plug into wired systems

- Wireless Network Concepts
  - o Introduction to Wireless Terminologies
  - o Wireless Access Points and Hotspots.
- Advantages of Wireless Networks
- Disadvantages of Wireless Networks
- Terminology in Wireless Networking
- Wireless Network Operation Modes

The popularity in wireless technology is driven by two major factors: convenience and cost. A wireless local area network (WLAN) allows workers to access digital resources without being locked to their desks. Mobile users can connect to a local area network (LAN) through a wireless (radio) connection.

- Converting Laptop into Routing Device
- Using one Data Card in more than one PC

For the same reason that WLANs are convenient, their open broadcast infrastructure, they are extremely vulnerable to intrusion and exploitation. Adding a wireless network to an organization's internal LAN may open a backdoor to the existing wired network. This section discusses some of the attacks that can be launched against a WLAN. These include eavesdropping, open authentication, spoofing,

- Wireless Attacks
- Concepts of WEP and WPA – WPA2
- MAC Address Spoofing
- MAC Flooding
- Eavesdropping
- WPA De-authentication Attack
- WPA2 De-authentication Attack
- Creating Rouge Wireless Access Point

Wireless networking opens up a network to threats that you may not ever even consider on a wired network. We need to fill up the Security Holes in Wireless Networks. This section will take you through the Security Practices which are needed for Wireless Security

- Wireless Defenses in Depth
- Changing the Default Settings
- Cloaking the SSID
- MAC Address Filtering
- Configuring a Strong WPA Key

Conducting scheduled penetration tests to verify the security of the wireless network are also recommended. Technology changes rapidly, as do the tools that hackers use to exploit it. A wireless network that was safe last year may not be as secure this year.

Website Exploitation

A website is a collection of related web pages, images, videos or other digital assets that are addressed relative to a common URL, in an Internet Protocol-based network. A web site is hosted on at least one Web Server, accessible via a network such as the Internet or a Private Local Area Network.

- Introduction to Web Servers
- Configuring a Web Server
- Making your Own Website
- Introduction to Database Servers
- The Web Login Process

Hacking of websites is resorted to by many hackers to get publicity and recognition for their deed. Website Hacking is not uncommon. It is simply trying to break into a site un-authorized.

Attackers can potentially use many different paths through your Web Application to do harm to your business or organization. Sometimes, these paths are trivial to find and exploit, and sometimes they are extremely difficult. Similarly, the harm that is caused may range from nothing, all the way through putting you out of business. Below we present a focused list of the Top Most Critical Web Application Security Risks.

- Web Application Attacks
  - o WebRipping
  - o SQLInjection
    - Input Box Based SQLi
    - Error Based SQLi
  - o PHP Code Injection
  - o Shell Injection:R57,C99,C100,etc ‘
  - o WebsiteDefacing
  - o CrossSiteScripting:XSS
  - o DirectoryTraversalAttacks
  - o Intercepting and modifying requests and responses

Whether you are new to web application security or are already very familiar with these risks, the task of producing a secure Web Application or fixing an existing one can be difficult. If you have to manage a large application portfolio, this can be daunting. You do need to follow some measures to secure your Web Applications.

- Putting breaks on Web Application attacks
  - o Proper Input validation
  - o Directory access controls
  - o Deny Google to your website

Web Application security is no longer a choice. It has become a necessity now. Between increasing attacks and regulatory pressures, organizations must establish an effective capability for securing their Web Applications.

Hack into Linux

Linux's functionality, adaptability and robustness, has made it the main alternative for proprietary UNIX and Microsoft operating systems. IBM, Hewlett-Packard and other giants of the computing world have embraced Linux and support its ongoing development. Well into its second decade of existence, Linux has been adopted worldwide primarily as a server platform.

- History of UNIX
- Introduction to Linux
- Advantages to Linux
- Different Versions of Linux
- Difference between Linux & Windows

If you're new to UNIX and Linux, you may be a bit intimidated by the size and apparent complexity of the system before you. At first glance, Linux looks a lot like MS-DOS--after all, parts of MS-DOS were modeled on the CP/M operating system, which in turn was modeled on UNIX. However, only the most superficial features of Linux resemble MS-DOS

- Basics of Linux
  - o Commands
  - o FileSystem o Kernels
  - o FileStructure

Linux is an Open Source Operating System with many vendors providing different security options. Unlike other OS, Linux is not so secure. Linux is optimized for convenience and does not make security easy or natural. The security on Linux will vary from one user to another user. Linux security is effectively binary; all or nothing in terms of power

.

- Linux Vulnerabilities
- Hacking Linux Login Password
  - o Modifying the Grub
  - o UsingLiveCD
  - o UsingTools
- Hacking Linux Networks
- Firewalls in Linux

In the ever-changing world of global data communications, inexpensive Internet connections, and fast paced software development, security is becoming more and more of an issue. Security is now a basic requirement because global computing is inherently insecure.

.

- Securing Linux
  - o Improve Login & UserSecurity
  - o Protect GRUB
  - o SetBoot Security Controls
  - o Secure the Network

Security involves defense in depth. Approaching security a step at a time, with consistency and vigilance, you can mitigate the security threats, and keep the crackers at bay