STL’s Modular certification program dynamic and static. course provides an in-depth to the tools and methodologies used to perform analyzing malware: code (Static) analysis and behaviour (dynamic) analysis. In research, etc. There are basically two broad categories of techniques that are used for malware analysis is used for forensics, honeypot research, security vulnerability repercussions, containing the incident and in planning recovery steps. Besides user’s access. This course aims in teaching the complicated analysis techniques Traditionally, malware analysis has been considered to be very complicated, and which, remediation efforts usually fails. manually and without relying on the automated scanning engines, without administrators to be able to determine if a binary is harmful by examining it which, remediation efforts usually fails. Traditionally, malware analysis has been considered to be very complicated, and in fact some of the techniques are still very complicated and beyond a normal user’s access. This course aims in teaching the complicated analysis techniques in a simplified manner and make a big learning curve for security professionals. This course helps in assessing the security incident scope, severity, repercussions, containing the incident and in planning recovery steps. Besides malware analysis is used for forensics, honeypot research, security vulnerability research, etc. There are basically two broad categories of techniques that are used for analyzing malware: code (Static) analysis and behaviour (dynamic) analysis. In most cases, a combination of both these techniques is used. This 2 / 5 day course provides an in-depth to the tools and methodologies used to perform dynamic and static.

Who Should Attend

This course will significantly benefit for those who is concerned about information security, Internet security, maintaining the integrity of operating systems, network infrastructure and other applications. This course will significantly benefit for IT Managers, Information Security Managers, Security Analysts, Security Consultants, Security Architects, Security Specialists, System & Network Administrators, Computer Security Incident Response Team member, Computer Forensic Investigators

About The Course:

Nowadays, the grown malware include network-aware worms, trojans, DDoS agents, IRC Controlled bots, spyware, rootkit etc., with infection vectors such as email harvesting, browser exploits, operating system vulnerabilities, and P2P networks to spread. It is essential for users and absolutely essential for administrators to be able to determine if a binary is harmful by examining it manually and without relying on the automated scanning engines, without which, remediation efforts usually fails. Traditionally, malware analysis has been considered to be very complicated, and in fact some of the techniques are still very complicated and beyond a normal user’s access. This course aims in teaching the complicated analysis techniques in a simplified manner and make a big learning curve for security professionals. This course helps in assessing the security incident scope, severity, repercussions, containing the incident and in planning recovery steps. Besides malware analysis is used for forensics, honeypot research, security vulnerability research, etc. There are basically two broad categories of techniques that are used for analyzing malware: code (Static) analysis and behaviour (dynamic) analysis. In most cases, a combination of both these techniques is used. This 2 / 5 day course provides an in-depth to the tools and methodologies used to perform dynamic and static.

Course Overview & Objectives

Malware, short for malicious software, is a programming code, scripts, active content, and other software designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior. The prevalence of malware as a vehicle for organized Internet crime, along with the general inability of traditional anti-malware protection platforms (products) to protect against the continuous stream of unique and newly produced malware.

The adoption of a new mindset for businesses operating on the Internet, acknowledge that some sizable percentage of Internet customers will always be infected for some reason or another, and that they need to continue doing business with infected customers. The result is a greater emphasis on back-office systems designed to spot fraudulent activities associated with advanced malware operating on customers’ computers.

Course Benefits:

The entire course provides step by step guided hands-on exercises that covers framework of malware analysis such as:

- How to set up controlled environment
- Lab for understanding the working of malicious software
- Learn to examine the program’s behavioral patterns,
- Learn to identify malware characteristics
- Learn the Process of Reverse-Engineering the binaries.
- Understand PE Headers and learn to work with PE Headers and DLL interactions
- Learn Import and Export Address Tables and usage
- Experiment the reversed code and learn the windows API use patterns
- Learn the program’s key components and execution flow
- Lean various executable packing and obfuscated programs
- Understand and learn unpacking techniques
- Learn the techniques for bypassing, with anti-analysis capabilities of armored malware

After the successful completion of the course, participants would be able to analyze an unknown binary and determine whether it is malicious or not. For those who require more in-depth knowledge should be able to reverse engineer the unknown/malware binary, understand and document its workings completely.

Course Outline:

Reverse-Engineering Malware Analysis Tools and Techniques training modules.

Module1. Introduction to Malware
Module2. History of Malware
Module3. Classification of Malware
· Virus-Worm - Trojan - Key Logger - Rootkit
· Backdoor - Downloader - Droppers- Injector
Module4. Methodology
· Creating a controlled environment
· Base-lining the environment
· Information collection - Information analysis
· Reconstructing the big picture - Documenting the results
Module5. Introduction to Windows Architecture
· Module6. PE headers of malicious Windows executables
· Module7. Dynamic Malware Analysis
· Monitoring System changes - Sandbox
· Tools for Behaviour Analysis
· Analyzing memory to assess malware characteristics
· Module8. Static Malware Analysis
· Core concepts for reverse-engineering malware at the code level
· Packers and Protectors - Rebuilding Imports
· Handling DLL interactions and API hooking
· Manual unpacking of protected malicious Windows executables
· Module9. Introduction to Dissembler
· Identifying the x86 assembly logic structures with a dissembler
· Disassembly of Malware samples
· Module10. Introduction to Assembly Language and command
· Module11. Anti-Reversing Techniques
· Module12. Exploits, Exploit Payloads and vulnerabilities
· Module13. Containment of the infected box
· Module14. Internet Searches
· Module15. Hands on Sessions
· Module16. Conclusions

About The Course:

Nowadays, the grown malware include network-aware worms, trojans, DDoS agents, IRC Controlled bots, spyware, rootkit etc., with infection vectors such as email harvesting, browser exploits, operating system vulnerabilities, and P2P networks to spread. It is essential for users and absolutely essential for administrators to be able to determine if a binary is harmful by examining it manually and without relying on the automated scanning engines, without which, remediation efforts usually fails. Traditionally, malware analysis has been considered to be very complicated, and in fact some of the techniques are still very complicated and beyond a normal user’s access. This course aims in teaching the complicated analysis techniques in a simplified manner and make a big learning curve for security professionals. This course helps in assessing the security incident scope, severity, repercussions, containing the incident and in planning recovery steps. Besides malware analysis is used for forensics, honeypot research, security vulnerability research, etc. There are basically two broad categories of techniques that are used for analyzing malware: code (Static) analysis and behaviour (dynamic) analysis. In most cases, a combination of both these techniques is used. This 2 / 5 day course provides an in-depth to the tools and methodologies used to perform dynamic and static.

Who Should Attend

This course will significantly benefit for those who is concerned about information security, Internet security, maintaining the integrity of operating systems, network infrastructure and other applications. This course will significantly benefit for IT Managers, Information Security Managers, Security Analysts, Security Consultants, Security Architects, Security Specialists, System & Network Administrators, Computer Security Incident Response Team member, Computer Forensic Investigators

About The Course:

Nowadays, the grown malware include network-aware worms, trojans, DDoS agents, IRC Controlled bots, spyware, rootkit etc., with infection vectors such as email harvesting, browser exploits, operating system vulnerabilities, and P2P networks to spread. It is essential for users and absolutely essential for administrators to be able to determine if a binary is harmful by examining it manually and without relying on the automated scanning engines, without which, remediation efforts usually fails. Traditionally, malware analysis has been considered to be very complicated, and in fact some of the techniques are still very complicated and beyond a normal user’s access. This course aims in teaching the complicated analysis techniques in a simplified manner and make a big learning curve for security professionals. This course helps in assessing the security incident scope, severity, repercussions, containing the incident and in planning recovery steps. Besides malware analysis is used for forensics, honeypot research, security vulnerability research, etc. There are basically two broad categories of techniques that are used for analyzing malware: code (Static) analysis and behaviour (dynamic) analysis. In most cases, a combination of both these techniques is used. This 2 / 5 day course provides an in-depth to the tools and methodologies used to perform dynamic and static.