

Introduction to Information Security

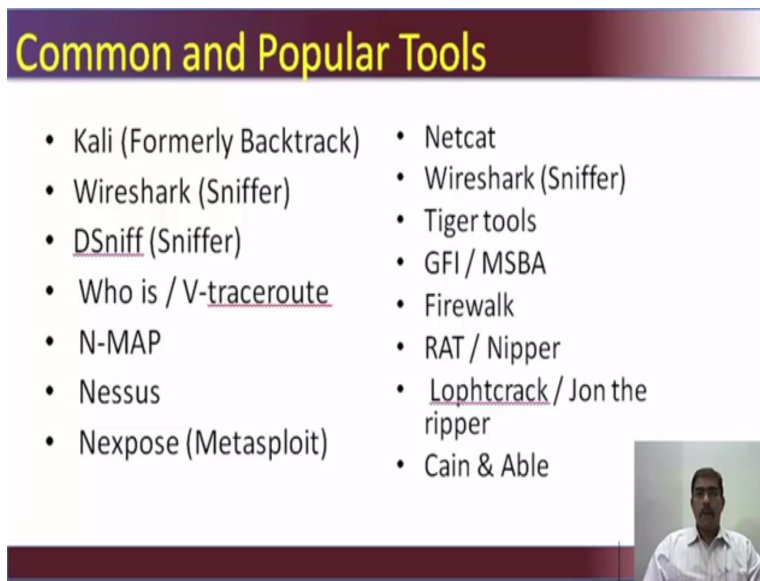
Prof. Dilip H. Ayyar

Department of Computer Science and Engineering

Indian Institute of Technology, Madras


Lecture - 48

(Refer Time Slide: 00:10)



Common and Popular Tools

- Kali (Formerly Backtrack)
- Wireshark (Sniffer)
- DSniff (Sniffer)
- Who is / V-traceroute
- N-MAP
- Nessus
- Nexpose (Metasploit)
- Netcat
- Wireshark (Sniffer)
- Tiger tools
- GFI / MSBA
- Firewalk
- RAT / Nipper
- Lophtrcrack / Jon the ripper
- Cain & Able



Now, let us take a look at some of the common and popular tools, used for penetration testing. Kali, which was called backtrack before, wire shark which is a sniffer, dsniff also sniffer, who is v trace route, n map, nessus, nexpose which used the metasploit, net cat, wire shark, tiger tools. Gfi, landguard, Microsoft base end analyzer, firewalk, a penetrating of firewalks, round audit tools nipper, its again audit tools for router and fire walks, Lophtrcrack, jon the ripper, cain and able.


There are hundreds of other tools, also available for conducting the vulnerability assessment and penetration testing. However, these are some of the popular tools, which you can try out, which you can learn, and these are very effective tools. We come to the end of this session, so we have learn about network security, we have seen the differences between vulnerability assessment and penetration testing, phases of penetration testing, what tools are used for penetration testing, and critical issues, differences between black box, bare box. Then some

of the popular tools, that are used for penetration testing, with this we go on to audits of different kinds.

(Refer Time Slide: 02:03)

Data center Audits

- Physical
- Environmental
- Power / backup power
- Access Control
- CCTV
- Network
- BCP / DRP
- Compliance
- Monitoring
- Responding to incidents
- SLA's
- Fire / Water



We come to data centre audits, now it is all very deep field, you generally go audit using, while using the methodology of interview, observation, to view a documentation, discusses. There are several areas that you have to conduct when you are doing an audit of data center. Right from physical, environmental, power and backup, access control, closed subject television cctv, network, bcp drp, compliance, monitoring, how the organisation of the responds to incidents, service validation with different vendors, fire and water.

(Refer Time Slide: 03:00)

- Fences and walls
- Locks
- Power-off switches
- Beta sites
- Backup systems
- Uninterruptible Power Supplies
- Properly designed forms
- Training and awareness programs
- Warning signs
- Reference checks
- Segregation of duties
- Surprise inspections
- Authorization schemes
- Employee identification badges
- Cipher locks
- Guards and guard dogs
- Network firewalls
- Compartmentation
- Fire-retardant materials and safes
- Anti-viral software
- Cryptography and key management



And fences and walls, the locks, the power off switches, beta sites, backup systems, UPSs, and forms, training and awareness programs, warning signs, reference checks, segregation and separation of duties, surprise inspections, authorization schemes, employee identification badges. Cipher locks, guards or guard dogs, network firewalls, compartmentation of security, or the organization itself, different areas, fire retardant materials, and safe, anti viral software, cryptography key management.

So, some of the areas have been highlighted here. Basically, when you do an audit of data centre, you do a walkthrough of the place first, of the infrastructure. So, you try to assess the physical security, by saying whether the guards, who are manning the building, are entering the details properly, whether any unauthorized entry can happen. Whether proper identification, visitor identification, badges are being issued, how long is the pass valid for the person.

Whether your mobile phones, your camera, laptops, are allowed inside the data centre, then you walk around premises, to see entry points, potential entry points, whether it is guarded. Whether cctv facility is there, to monitor to perimeter of the data centre or where the data centre is situated, whether anybody can just jump over and get inside the premises.

So, in physical access, as first level, you will see the fidelity of security, the guard, then you go in inside, you see, whether there is a reception, whether the visitor are controlled, whether the access control or physical access control mechanisms are in place, to restrict the entry of only authorized people. Whether employee is parking the visitor to his or her cabin, or to the bathrooms, whether proper proximity cuts inside your biometric is installed.

So, in physical access, you cover up all of these aspects, so when you visit the data central, the points can be added or subtracted depending up on the infrastructure under which in data central secreted. Similarly, you see environmental controls, whether effect oriented fire extinguisher is in place, whether there are proper exit signs, for immediate evacuation of the personnel, whether smoke detectors are present, whether the fire extinguishers themselves have validity period written on them, whether it is tested properly.

Then, whether water detectors are installed below the data centres for you, and then anti static tiles have been put in the data centre, then you have temperature and humidity control, whether procession air can be recognized or no. How it is operated, what are the

maintenance schedule for that, whether a backup format is available. So, these will come under environmental control, also whether proper warning signs are put.

For example, no eatables allowed, inside the data centre. Then emergency contact numbers. People who are the trained in use of fire extinguishers, or evacuation, whether that is described properly, whether proper security guidelines have been posted, whether the exit signs have been clearly marked. Then, we go on to a logical security, how users within the infrastructure are accessing loop source ,what was the security level there, then you see the password complexity, password link, password history.

So, moving the logical access controls, then you also see whether proper position is made for UPS, whether backup generator also available, in case of prolonged power surges, then you can see the communication lines, alternate diverse routing how is it available similarly, for the power. Then you see, after the communication line, where it terminate, whether load balances are there, whether it is terminating to the fire wall, and whether there is proper control is there over the firewall itself.

From there to the servers, who get access to what, whether free access is given to the server from the internal network, or is it through turbulated through the moves up, or user name and password. In many places, you see that RTP is used wherever windows are used, the credentials are stored in the desktop. So, user just has to give the ip address and then directly login in to, that is a bad practice.

So, we will have to see what kind of controls are implemented , within the infrastructure segregation and separation of duties, is another important aspect. Your system administrator and auditor cannot be the same person, as an example. So, then whether are, an employee wearing the identity identification badges, in factors there you can distinguish between an insider and an outsider.

How many firewalls are there, what is the backup for the firewall, how the configuration changes are needed, who operates the configuration manuals, then reviewing the rules of the firewall itself, whether it is done properly. Then, compartmentation is whether it is a big hall, where all the department were mix up, or where is compartmentation utilization of department, where IP has access, based on a different VLAN, connected to the data center.

The HR and admin itself, they do not have access to what IT has, existence of antivirus software, and if cryptography is used, how the peek management happens. So, data centres audit itself is, whatever we have learned, right from domain one, all are those put together will be a data centre audit, and with including the spoken intrude or vulnerability assessment, and penetration just an technical infrastructure also.

Some of the data central audits will extensively depend, upon usage of check lifts dependent on, so many items to be seen. There are checklists available in an internet. But then you will have to take it, customise it, to the Indian environment, number 1, and also customise it to the organisation, that you will be auditing on. There may be several aspects, which may not be possible to implement, it may be a shared resource, where it is not or the infrastructure, is not owned by the organisation itself.

So, your check list will change, also check list will give you an idea, or it will remind you that, you have revisited or visited this point, or visited this aspect. So, it is a very important document for you to carry, when you are going for a data centre audits. Again the check list will have summary, of whatever we are formed, you will find, or you will read the security policy, see whether points covalent to physical access are being followed.

You see the procedure for that, and check for its relevancy, and currency. Whether it is correct, or else anything has to be changed in cctv. If we see yes it is been recording, but who verifies it, there is nobody to monitor, that is an issue. Then again, when you talk about log management, whether proper SIM tool has been used, whether analysis is done, whether there is a security operations unto itself monitor security issue within the organisation, whether a web application firewall has been installed to protect the website.

If the organisation monitoring the attempted inclusions, so there are several aspects, that you will move to determine a security, or to audit a data centre by use all usage of check list, use in a innovative measures, use social engineering techniques, to see whether you can penetrate into the first level, second level, third level.

So, there are different ways or different methods, you have to follow to, do a data and audit, to also have to check, and the importance of information security awareness inside the organisation. So, you will see whether employees working there, have been trained adequately, do they understand the implication of a breach, and what measures they have to take as users to protect the organisation infrastructure, from such intrusions.

How frequently is the training given, whether is it a part of only the new employee orientation, or is it conducted on a regular basis, then whether the background verification, or reference checks are done for any employee, who is been appointed, within the organisation. So, that should be elaborate proper process. Authorizations schemes whether it is followed.

Now, we need to access the server using this, this and this method, or it can be a user name, it can be a password plus token, or password plus two factor of authentication, some of the tools have two factor of authentication methods. So, you need to understand how we organisations works, what are all security measures they have implemented, and then conduct the audit based on that.

For example, when you do an audit of a bank's data center, it will be much different that if you do audit of the data centre of an airport. Now, that criticality of information, the aspects of confidential, integrity of availability, It differs for different organisation is doing different businesses, for a bank confidentiality of information is important, integrity is also important, availability is also important.

For say a pharmaceutical company, confidentiality is important integrity is also a very high important, integrity a little more, because the composition of drugs that are made. So, similarly, for different organisation, different level of security, which are required some aspect may be more crucial, than the other. So, you need to understand, how the organisation works, what are the CIA requirements, and then the do audit on this.

Sometimes, I have seen in the data centres itself there is a poster, or there is a big framed certificates rating that, they are 27001 compliant, PCI DSS compliant, or 9001 2008 compliant, but when you actually go, and see the documentation, you may find that yes they do have documentation. For that purpose of satisfying a standard, and or a requirement. But then, it is not comprehensive.

The standards says you have to implement point 1 to 10, but then your security may requirements may say that you need points 11 to 25 also, you may find point 1 to 10, but then 11 to 25 should also be covered. It should give the auditor a false sense of hope that everything his in space, because your organisation 27001 certified or 9001 certified or any other standard certified.

So, comprehensive audit needed to be done. You have to assume that, organisation has everything, and yet nothing. So, you should have an attitude which says that, yes I need to find out all these aspects within the infrastructure, so that the recommendations can be correct, and as an auditor or an assessor, you are working for improving the security of the organisation.

It is not for a personal benefit, so you need to be more diligent, you need to practice new things, you need to bring out the facts, and as you see them. The reporting also plays a major part, you can write that xyz is not there, or xyz aspect. Can you improve again, it depends on how you want to convey your talks, to the management, to improve the information security process.

You should make the employee, within the organisation understand that, you are doing it for improving the overall security, and it is not a fault finding exercise. Many of the audits say, because the employees internally within the organisation, do not cooperate as much to the auditors, and generally are the people to direct auditors to say to bribe in a particular way, if you do not write the audit report in this particular way next time, we are not going to get your work.

This is an actual practical situation that I have encountered so many times, but when like we discussed earlier, audit in an Indian scenario is done only with the intention of complying with some guideline, or the other and not for actual improvisation, or improvement of security. The top management fails to understand that, the senior management fails to understand that, the people who managed or maintain the network, they fail to understand that, because they fear that, if there is a vulnerability which is reported, then management may take strict actions including termination of a job. So, it becomes difficult for the auditors when they do big audits, because the objectivity should not be lost. Auditor should try and tell the employee, and make them understand that it is done to the benefit of the organisation, and not for an individual or personal benefit.

So, your data centre audit, again it revolves around usage of check list. You can make your own check list, or there are several check lists available but, be sure to modify them, as per the requirement of the organisation. The environment in which it is operating, and compliance requirements that may be applicable to the organisation. These points effectively

will guide you , or will help you understand what a the data centre audit is. It covers right from you physical, to your incident management.