Penetration 101 - Introduction to becoming a Penetration Tester

Dave Burrows

Dave Burrows
GIAC Security Essentials Certification (GSEC) Version 1.3
Penetration 101 – Introduction to becoming a Penetration Tester

Overview

The purpose of this paper is to give you a brief and basic overview of what to look for when starting out in penetration testing and to build up an internal penetration test kit to aid you in performing both internal and external penetration tests on your company network. To also make you aware of the problems with new network technology like wireless networks, and remote access devices that can circumvent network perimeter security devices like firewalls and IDS. Whilst also showing you the pit falls of security, and the need to check all systems for vulnerabilities and to carry out regular patching and monitoring of all systems within your network. This paper also lists suggested well known security penetration tools for both Linux and Windows operating systems.

Introduction

Over the past two years we have been hearing in the news about many more Denial of Service attacks on high profiled companies like Yahoo and Microsoft. We have also been hearing that hacking attacks and website defacement are becoming more frequent and are happening to thousands of companies worldwide. Time has come where we need to protect ourselves from everyone out there be it our company rivals, the seasoned hacker or just Joe Bloggs teenager down the road. We need to protect our company's infrastructure like we do with our homes and personal property. Two to three decades ago, people would be quite happy to leave their houses and cars unlocked, and even doors to their houses left wide open due to low crime levels. Time is constantly evolving and the world is getting a much worse place to live and work in. To better protect your network you need to know about current and past vulnerabilities and patch all equipment as soon as vulnerability patches are made available. However this alone will not protect you. Everyone is human (or at least in this day and age), and we all make mistakes. Whether it's granting full access permissions to a server by accident, to not setting a password on the administrator account because it makes life easier for us to manage. No matter how much patching you do to your environment; the systems can still be vulnerable to attack. This is where Penetration Testing comes in.

Hackers and other people who might want to get into your network will perform attacks on your systems. You need to find what they do and to perform these same sorts of attacks to try and attempt to penetrate your network and to locate compromised systems.

What is Penetration Testing

Penetration testing involves performing various reconnaissance scans against your perimeter defenses, boundary routers, firewalls, switches, network devices, servers,

and workstations to allow you to see which devices are within your environment and to determine the overall plan of the network and topology. Once this has been gathered, you can then collate this information and then look at an attack vector to try and penetrate identified systems to see if they can be compromised by using known vulnerability scans, attacks and denial of service attacks. When performing penetration testing you are essentially taking on the role of the hacker. You will be looking at using tools like PING to detect if hosts are live, port scanners for any hosts that may deny ICMP Echo/Reply requests (PING's) and to also identify which ports are open on devices enabling you to create a footprint of what these devices are used for. (10)

The overall plan is to map out the entire network and to make sure any vulnerable devices are known and patched frequently.

Why do we perform Penetration testing

Hackers like to spend most of their time finding holes in computer systems where mostly bad coding are to blame in creating vulnerabilities. Hackers then like to take this knowledge and apply it to real world scenarios by attacking your network. They may be doing this as a grudge because they weren't hired by your company, or perhaps was fired at some stage or even they don't like your company, or just want to get a Kudos kick out of saying, been there, done that! To try and protect our computer systems from these hackers, we need to check for known vulnerabilities and exploits ourselves within our systems. Vulnerabilities can comprise of bugs, application back doors, spy ware that have entered into the coding of the application, operating system or firmware at development time of the product or files that have been replaced at a later date in the form of viruses or Trojans.

Over the past two years we've seen many hackers performing denial of service attacks against ISP's (1), Banks (2), and even world governments (3). Carnegie Mellon Software Engineering Institute a Computer Emergency Response Team (CERT) and many other CERT's collate known and new vulnerabilities across all systems, platforms and applications and publish these to the security community and to the companies who have created the systems in a hope that people will become more aware of vulnerable systems and also to allow the creator's of these products to create and distribute patches for their products. In the event of a patch taking a while, in most cases a technical work around is published to harden the systems that may be affected by this vulnerability.

Who should perform Penetration testing

Most auditing companies now provide some level of Penetration testing either from within their company, or sub contracted out to third party security companies. If your company would like a penetration test performed on your current infrastructure, you can outsource to one of these companies to perform tests.

Many companies are now looking at creating their own internal security teams that provide a constant day-to-day monitoring of networks and devices, and also spend valuable time researching the latest vulnerabilities from CERT's and collate the relevant security patches in-house under advisement from the Security Community to apply to company systems that are deemed vulnerable or compromised. Unfortunately even if you are patching systems you will always be one or two steps behind the hackers and this is unavoidable, but it's much better than being 20 or 30 steps behind them by failing to identify and patch your systems and becoming vulnerable to attack or even worse, allowing your networks to attack other companies networks which is now in the process of being made illegal in several countries. The UK government are already looking at making it part of UK law that you will be fined if you are found attacking other companies or systems on the internet unless you can provide proof that you are taking security seriously within your organization and applying all available patches regularly to try and stop future attacks from happening. The UK government is also trying to push more responsibility onto ISP's, so that ISP's should be looking out for attack vectors, and if they find attacks coming from their customers or within their networks, they are at liberty to cease infected services until the system is made safe.

Penetration testing can be performed by anyone who is either knowledgeable in this area and keeps up to date with the latest security news, penetration applications and researching ways of attack, or has had extensive experience on penetration system testing or is certified.

Outsourcing

Outsourcing penetration testing can be a very costly exercise and one that you might want to only perform once a year. The problem with most networks is that they are constantly changing. People move equipment around the office or between office locations and also install software on PC's and servers, so penetration testing only gives you a snapshot of compromised systems at that moment in time to give you a guide. You also have to be extra vigilant when employing a security testing company. You need to make sure they have liability insurance! Do they come with certified security credentials? (4) Do they bait and switch ? (5) or do they employ real life hackers which have their own agenda ?

My Network is secure!

"I understand all of what you have said, but my network **IS** secure, why should I authorize spending all this money on checking our network when it is not necessary?" The simple answer is ***insecurity***. You may think you are secure, but in most cases companies find that once they have had their first penetration test performed that most of their personal, private and highly confidential data is or can be compromised very quickly and in some cases left wide open for anyone to view, even your closest competitors! People around the world prior to September 11th 2001 believed even though there were wars happening across international borders, that each country was secure within it's own territory. September 11th showed us that absolutely nobody is

secure. Be it from a terrorist stand point from allowing bombs, plastic explosives and terrorists onto planes which can be easily hijacked, or to securing our networks from these same class of people or hackers who stealth themselves online which are now taking war to the next level – Cyber Crime and Cyber Terrorism.

My network isn't connected to the Internet, so why should I worry?

Attacks don't just come from the Internet. Although the majority of attacks do, you will find hackers running programs called war dialers to target telephone exchanges within your company, dialing in remotely to your network remote access points, or some hackers have the plain nerve just to walk into your offices, sit down at a workstation and start working from there. You can even find your own staffs are trying to hack into internal servers to look at sensitive company data like payroll. If someone came into your office and sat down at a vacant desk with a computer on it, would you get up and ask who they are and tell them to leave? Most people don't, because they prefer to avoid conflict. They would just happily assume this person has been brought into the company as a contractor, an installer or perhaps a new member of staff. Also be aware as technology is still evolving at a terrific rate that many companies are now adopting wireless networks. There has already been a case where RSA Security drove through the City of London armed with only a laptop, wireless network card and some free software downloaded from the internet and found it could pick up the traffic on dozens of corporate WLAN's, 'leaking' out of buildings which could invariably allow them to grab companies data without anyone in that company knowing. There have been a few substantiated reports that even an empty tin of Pringles will make a good wireless antenna/receiver (6,7,9)

Pringles DIY antenna / receiver [6]

My network's connected to the Internet and has a firewall so I'm protected!

Does anyone in your company apply regular patches and perform penetration testing? I've spoken with IT managers from many companies and the first thing they say when you mention security is "we're protected because we have a firewall" or "we have an intrusion detection system in place, so sure we're protected, right?"(8). In recent statistics provided from the UK government show that UK company's top priority is

[6] Ward

now security. However, only a quarter of these same companies have a decent enough security policy in place to cope with potential security problems such as viruses, hackers and other cyber pests. It's like saying I've got a 10 bolt lock fitted to all my doors in my house and have an intruder alarm, but I never switch the alarm on, and I always leave the doors unlocked and ajar because I trust people will not come into my home and steal anything. If you're going to install a firewall, IDS, or NIDS you need to be able to go the full mile.

Most IT managers still fail to realize that they can have the latest all singing and all dancing firewall or IDS (Intrusion Detection System) in place, but just like operating systems and servers, if you don't keep it patched or filtered for the latest known vulnerabilities, or even configured to monitor for irregular patterns in traffic then they've just bought a very expensive paperweight. Firewalls, IDS and NIDS (Network Intrusion Detection Systems) are in constant need of attention and monitoring. They only do what you ask them to do, so you should either be looking at having an in-house team dedicated to configuring, and monitoring the complete network or this should be outsourced to a security or networking company who deal with installations and on-going configurations of these devices on a daily basis.

Monitoring the hacking community and get into their way of thinking

Most hackers will start off as what is more commonly known as script kiddies. They modify other peoples code to see what happens, and evolve from this. Get into their mind by thinking like a hacker. (11)

Visit the newsgroups where some hackers hang out, search the Internet for hacking websites. Scan through some of the online forums where hackers may hang out and read and watch what hackers are using, keep an extensive log of where you've been by book marking relevant sites into various categories (this will help you return at a later date), and download any programs you think might help either hack or test a system for vulnerabilities, or even crash a system by various Denial of Service attacks. These will all come in handy in your testing.

Hacking websites disappear off the net very quickly, mainly because most of them have tools that are deemed illegal by most Internet Service Providers or companies who have the vulnerability in their product. So if you find a good site, don't lose it! Take a backup of the site either with Internet Explorer or Netscape Navigator with their saving to disk cache options, or use an offline web cache creator to traverse the website and download it to disk. This may take a while if you are running from a dial-up modem, but this way the website is always accessible in the future to you, and at a fast speed!

The ultimate goal to penetration testing

The ultimate goal is to see how secure your network is or from a hacker's point of view, how insecure your network is currently. You need to be able to test all systems that are on your network, no matter which operating system or application they run.

If there's one thing you need to remember it's this… **ALL SYSTEMS ARE VULNERABLE!** Some more than others, but no system is ever 100% secure either now or in the future. If your network hasn't had any penetration tests performed, and you don't consistently patch all hardware, operating systems and applications with the latest security patches then you could find your network being a massive target for attack. To penetration test you will need to scan your systems both internally and externally to see what information you can get back. Hackers will want to get at devices on your network; most will probably be doing this from the Internet, or trying to dial in to your remote access servers. Do you have any dial-up modems attached to desktop PC's and phone lines? If so, try dialing into these and performing penetration testing. Some hackers may just want a kudos kick to say "Hey I've been there and done that", and post it up to some of the hacker sites or defacement sites to show how good they are. Some will want to get at your personal data for their own use, sell it on or perhaps use it for blackmail or perhaps for industrial espionage.

The testing you will be performing will show to what extent your systems are at risk so you can pro-actively gain support from management of which is very important and allow you to start putting together a security policy and a patching schedule of systems. This patching schedule should not only be for core systems, but all systems! Do not leave any stone unturned. If you have test PC's on your network, patch them! Don't leave them so they are still vulnerable. If you just have one or two devices that are vulnerable on your network, these could be used to spread viruses, Trojans and other hacking programs or allow a hacker into your system and to compromise other cleaner systems.

Systems check list

Inventory all devices within your network. This includes hubs, network switches, email, proxy, Internet servers, DNS, Domain controllers just to name a few. Talk to the teams within your organization that manage these as they may have already done this to a high level you require. Correlate all of these together (I suggest using a spreadsheet), as this will become very large, very quickly and spreadsheet programs are good at managing this sort of information. Make sure you include the device name, IP address, and MAC Address, operating system, whether or not it's a server, and also what it's primary and secondary function is. Also which software does it have installed? This will then create a foundation for you and to allow you to start researching tools to test each of these environments. Make sure you keep this spreadsheet secure. This will become a very important working document and you do not want this to fall into the wrong hands! If once you've penetration tested these devices you find that half of them are running web servers like Microsoft Internet Information Server 5 when they shouldn't be, then uninstall these applications. (10)

Research Vulnerabilities

Search for Security Vulnerabilities, Incident Response, and Security Advisories in two or three of the top Internet search engines. You will probably want to visit at least the first 50 websites in each search you perform. Do any of these sites have lots

of information on them relating to various operating systems and applications? If so, bookmark these so you can return later. Make sure you create a category structure in your bookmarks, so you don't mix up Viruses with Security Vulnerabilities or Port scanning. The object of this exercise is to create yourself your own library or mini search engine of websites that may help you further in your security role.

Vulnerability patches

You will need a full list of vulnerabilities and patches that are available for each type of hardware, operating system and application you have on your network. A good start would be to visit CIAC – US Department of Energy Computer Incident Advisory Capability (http://www.ciac.org/ciac/bulletinsByType/bul_vendor_list.html) as this will give you a basis for what patches are available from different vendor's in a one view site. Also visit the vendor sites as most of these now have security areas too. You might want to check out Microsoft Security (http://www.microsoft.com/security/) and CISCO PSIRT Advisories (http://www.cisco.com/warp/public/707/advisory.html) to just name a couple. These will become invaluable websites and you will find yourself returning here on a regular basis.

Creating the Penetration Test Kit

1. Test Environment

Set up a test environment creating a network of multiple devices. Penetration testing can be very dangerous to systems if you start using hacking tools or are experimenting. This is why it's best to only test these on a test environment before using them against real-life devices. You may also find that some of the tools you have downloaded contain a virus or other Trojan code planted within the installation scripts or programs. Make sure you are running at least one of the top antivirus programs that are fully up to date. Scan the programs before use. Also make sure you've scanned for Trojans (most antivirus products don't scan for all known Trojans!). Try a program like Pest Patrol (http://www.pestpatrol.com), scan your entire test environment (including within compressed files). Discard anything that may have a virus or Trojan, and see if you can locate a clean version of the program you found. If not, discard the program, as it will probably do you more harm than good! Using a test environment is key to penetration testing. This way you can avoid scanning, attacking or creating denial of service attacks on production network devices within your company when getting to grips in learning how to penetration test.

2. Hardware

You should now be ready to start creating your Penetration Test Kit. You will need 3 or 4 PC's of approx 300Mhz or faster with as much ram as you can afford because you will be installing multiple operating systems and applications onto these devices that you have in your real world network. If you prefer to go the VMWare (http://www.vmware.com) route, which is highly regarded then you will require a fast

PC, greater than 1Ghz and have 512mb or greater. Most modern day laptops come with this specification and would be ideal if your networks are split over multiple sites, because you can then take your entire penetration kit with you and test from multiple networks rather than having it tied down to one location. VMWare will allow you to emulate a PC environment in a window from an operating system and software perspective. You can run multiple workstations and servers within this Virtual Machine environment and keep it off the company network, but still have the Virtual Machines networked with each other. VMWare also allows you to undo the changes since last power on, so if you've managed to crash a virtual machine and it won't restart, power it off and discard changes since last power on. It's a very powerful application; a very fast emulator and will save you time having to rebuild your test environment when it crashes. Do not underestimate it!

3. Operating Systems

You will need to have basic fundamental knowledge of both Linux and Windows. Enough to build the operating systems, log in as administrators and configure hardware like network cards and install and configure software. The majority of security tools are found on Linux, although in the past few months I have seen an increasingly larger selection of these tools being ported to Windows platforms.

4. Researching Security tools

You will need to spend a lot of time surfing the Internet for security tools. Once you have spent what seems like weeks and weeks of extensive research, you will see some of the same tools reappearing time and time again. What does this tell you? Probably that these tools are a popular tool used by the security community, and that they are likely free or very cheap. Most of these security tools are written by security consultants to better automate testing of systems to make their life easier. You will find that the security community continuously updates these applications as more vulnerabilities are discovered. Think for a moment, if you're using these tools to penetration test your network, it's most likely that hackers are also using the same style of tools! So this will give you a better understanding of what hackers are actually using out in the wild.

Make a note of each application you come across. Before long you will have a short list of probably two to three dozen packages, some running under Microsoft platforms, and some running under Linux/Unix platforms. Most of the best security analyses tools on the Internet to date are written to run under Linux and Unix based systems. The main reason for this is that the network stacks are more interoperable and generally have better performance than tools that are written on Microsoft platforms.

5. Recommended Tools to research

- Redhat 7.2 Enimga Linux
  http://www.redhat.com

RedHat if installed from CD or DVD and is very easy to install for the Linux novice and will give you a guided GUI setup program and will have you up and running with a KDE or GNOME X-Windows interface very quickly. If you are a Linux novice, then this would be a good Linux operating system to choose and contains lots of built in help systems and help forums that are available on the internet. Most security tools are available pre-compiled for RedHat so you won't have to get your hands dirty in re-compiling Unix source code and libraries. You will need a Linux platform to install some of the Linux based security tools.

- Windows 2000 Professional Workstation or Windows XP Professional
  http://www.microsoft.com/windows2000/professional/
  If you prefer or are happier with using Windows, then a Windows 2000 workstation will get you up and running allowing you to use a handful of security tools written for Windows based operating systems.

- Trinux
  http://trinux.sourceforge.net
  Trinux is a good command based Linux operating system that comes on a floppy disk and installs itself into RAM with a RAM Drive. Trinux brings together a comprehensive list of command line based security tools built around a Linux operating system. You can also download extra modules that can be downloaded on each boot from the Trinux website and installed into RAM for the current session. An ideal solution if you need to move around to multiple offices, prefer a command line interface over a GUI interface and would prefer that you have everything configured for you or if you want to run on a low specification computer.

- LanGuard Network Scanner
  http://www.gfi.com/languard/
  A fairly good port scanner for Windows and free!

- Nmap
  http://www.insecure.org
  Nmap now comes in two flavors. One version for Linux and one for Windows. The Linux version has better performance but either will allow you to run regular port scans to advanced stealth port scans to try and by-pass firewalls without being detected.

- Superscan

http://www.foundstone.com/knowledge/proddesc/superscan.html
A reasonable Windows port scanner. This will only perform TCP port scans (which are regarded as somewhat "loud"), where as other tools like Nmap will also give you better UDP port scans allowing for stealth scans. It can be a quick tool to run up if you want to scan something internally and not have to worry about being in stealth mode.

- Nessus
  http://www.nessus.org
  Nessus is a complete security scanner and vulnerability database for Linux, which is free and gives you free updates to the knowledge base on a regular basis. This will allow you to configure scans against network devices and pick and choose what style of scan or attack you would like to perform. Nessus also utilizes other great penetration tools like Nmap giving you full reports on your environment and links to potential security fixes or work arounds. You can do anything from simple port scanning to IIS or Operating System Denial of Service scans. This is a must have tool for every Pen test kit!

- SNMP Ping
  mailto:snmptool@sans.org
  SNMP is always a major vulnerability and easy configured by accident on most network devices. This tool allows you to scan subnets very quickly and determine which devices have SNMP switched on and which SNMP traps are available.

- Ethereal
  http://www.ethereal.com
  A good network protocol analyzer for both Linux and Windows running your network card in promiscuous mode allows you to sniff and capture data that flies past your workstation allowing you to examine packets and see what data is being transmitted across your network. A very good tool!

- Ettercap
  http://ettercap.sourceforge.net
  Another network sniffer for Linux, but also works over a switched network (where most network sniffers cannot) and is very good at what it does.

- TCP Dump
  http://www.tcpdump.org
  Another network analyzer for both Linux and Windows. This is a command line based tool but can be very quick to write the

contents out to file to examine network packets if you are in a hurry in capturing some network data.

Conclusion

You should now have basic knowledge of how a hacker will work to penetrate your network, what he will be looking for on your network and how to better protect yourself against future attacks. Remember to keep your environment fully patched and to perform penetration on a regular basis. Every 2-3 months would be a good starting ground and will make you aware of new systems that have been installed on your network without your knowledge.

References:

1. Heikkila, Pia, "Hacked ISP shuts down". Silicon.com, 22nd January 2002. http://www.silicon.com/a50624 (last accessed 30th April 2002)

2. Heikkila, Pia, "US Banks a major target for hack attacks". Silicon.com, 23rd January 2002. http://www.silicon.com/a50676 (last accessed 30th April 2002)

3. Hayday, Graham "US Government sites hacked by 'Mujihadeen'". Silicon.com, 3rd December 2001 http://www.silicon.com/a49633 (last accessed 30th April 2002)

4. Moyer, Philip R. "What to demand from penetration testers" (2002) http://www.gocsi.com/penet.htm (last accessed 30th April 2002)

5. eSec Consulting Services, "Penetration Testing Services" http://www.esec.com.au/ecs/images/pentest_may01.pdf (last accessed 30th April 2002)

6. Ward, Mark "Hacking with a Pringles tube", 8th March 2002 http://news.bbc.co.uk/hi/english/sci/tech/newsid_1860000/1860241.stm (last accessed 30th April 2002)

7. BBC News "Welcome to the era of drive-by hacking", 6th November 2001 http://news.bbc.co.uk/hi/english/sci/tech/newsid_1639000/1639661.stm (last accessed 30th April 2002)

8. Kerridge, Suzanna "Lax security shaming UK businesses" Silicon.com, 16th April 2002 http://www.silicon.com/a52714 (last accessed 30th April 2002)

9. Ludlow, David "Once you crack – you can't stop", 3rd april 2002. VNU Network News magazine

10. Scambray, Joe and McClure, Stuart "Hacking Windows 2000 Exposed Network Security Secrets & Solutions", 2001. ISBN 0-07-219262-3

11. Brenton, Chris, "Mastering Network Security" Sybex, 1999. ISBN 0-7821-2343-0

Addendum – other useful security related websites

- Security News related Sites
  - http://www.Incidents.org
  - http://www.theregister.co.uk
  - http://www.silicon.com
  - http://www.security-protocols.com/index.php

- New Vulnerabilities
  - http://bugtraq.inet-one.com/
  - http://www.cert.org/nav/index_red.html
  - http://www.microsoft.com/security
  - http://www.ciac.org/ciac/bulletinsByType/bul_vendor_list.html

- Advisories
  - http://www.cisco.com/warp/public/707/advisory.html
  - http://nsa2.www.conxion.com/

- Firewall information (seeing the wood from the trees)
  - http://www.robertgraham.com/pubs/firewall-seen.html
  - http://www.snort.org

- Hacking
  - http://www.webstore.fr/webabonnes/tahiti/nt.htm
  - http://www.cavebear.com/CaveBear/Ethernet/vendor.html

- TCP Ports
  - http://www.chebucto.ns.ca/~rakerman/port-table.html
  - http://www.iana.org/assignments/port-numbers
  - http://www.tsmservices.com/masq/
  - http://www.ec11.dial.pipex.com/port-num.shtml

    - http://www.stengel.net/tcpports.htm

- Securing
    - Microsoft Internet Information Server 4 Checklist
      http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/iischk.asp

    - Securing Microsoft Internet Information Server 5 Checklist
      http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/iis5chk.asp

    - Securing Microsoft Windows NT4 Domain Controller Checklist
      http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/dccklst.asp

    - Securing Microsoft Windows NT4 Member Server Checklist
      http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/mbrsrvcl.asp

    - Securing NT4 C2 Configuration Checklist
      http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/c2config.asp

All of the above website links were last checked for availability on 30th April 2002.