NETWORK DEFENSE GUIDE

NOTES from Hacking Exposed 7: Network Security Secrets & Solutions

Abstract

Casing the Establishment, Endpoint & Server Hacking, Infrastructure Hacking, Application & Data Hacking, Countermeasures, Appendix

Ivan V. S

2017

Contents

Part I: Casing the Establishment

1. Footprinting

What is footprinting?

- Gathering information about your target. Scoping the target interest to understand everything there is to know about that target and how it interrelates with everything around it, often without sending a single packet to your target.

Table 1-1: Tasty footprinting nuggets that attackers can identify

Technology	Identities
Internet	Domain Names
	Network blocks and subnets
	Specific IP addresses of systems reachable via internet
	TCP & UDP services running on each system identified
	System architecture (i.e. Sparc vs. x86)
	Access control mechanisms and related access control lists (ACLs)
	Intrusion-detection systems (IDSs)
	System enumeration (user and group names, system banners, routing tables, and SNMP information)
	DNS host names
Intranet	Networking protocols in use (i.e. IP, IPX, DecNET, etc.)
	Internal domain names
	Network blocks
	Specific IP addresses of systems reachable via the internet
	TCP & UDP services running on each system identified
	System architecture (i.e. Sparc vs. x86)
	Access control mechanisms and related access control lists
	Intrusion-detection systems
	System enumeration (user and group names, system banners, routing tables, and SNMP information)
Remote Access	Analog/digital telephone numbers
	Remote system type
	Authentication mechanisms
	VPNs and related protocols (IPsec and PPTP)
Extranet	Domain names
	Connection origination and destination
	Type of connection
	Access control mechanism

Why is footprinting necessary?

- It gives you a picture of what the hacker sees. If you know what they see, you know what potential security exposures you have in your environment. When you know the exposures, you can then prevent exploitation.

Basic Internet Footprinting Methodology:

1. Determine the scope of your activities
2. Get proper authorization
3. Publicly available information
4. WHOIS & DNS enumeration
5. DNS interrogation
6. Network reconnaissance

It is important to remember to minimize the amount and type of information leaked by your internet presence and to implement vigilant monitoring.

---

2. Scanning

What is scanning?

- If footprinting is the equivalent of casing a place for information, then scanning is equivalent to inspecting the walls for doors and windows as potential entry points.

Scan	Technique
Determining if the System is Alive	ARP Host Discovery
	ICMP Host Discovery
	TCP/UDP Host Discovery
	TCP & UDP services running on each system identified
Determining Which Services are Running or Listening	TCP connect scan
	TCP SYN scan
	TCP FIN scan
	TCP Xmas Tree scan
	TCP Null scan
	TCP ACK scan
	TCP Windows scan
	TCP RPC scan
	UDP Scan
Detecting the Operating System	Making guesses from available ports
	Active stack fingerprinting
	Passive stack fingerprinting

LEARN NMAP -- https://nmap.org/

Learn how to manage scan data with Metasploit -- https://www.metasploit.com/

---

3. Enumeration

What is enumeration?

- Enumeration involves active connections to systems and directed queries, it is very intrusive. Enumeration techniques tend to be platform-specific and are, therefore, very dependent on information gathered from scanning.

Use NMAP for scans, use tools like Nessus for vulnerabilities -- https://www.tenable.com/products/nessus-vulnerability-scanner

Be aware of:

Risk	Description
Fundamental OS Architectures	Windows NT Family's SMB underpinnings make it easy to elicit user credentials, file-system exports, and application info. Lock down NT and its progeny by disabling or restricting access to TCP 139 and 445 and setting RestrictAnonymous (or the related Network Access settings).
SNMP	Designed to yield as much information as possible to enterprise management suites, improperly configured SNMP agents that use default community string such as "public" can give out this data to unauthorized users.
Leaky OS Services	Finger and rpcbind are good examples of programs that give away way too much information. Disable programs such as finger, user secure implementations of RPC of TCP wrappers, and find out from vendors how to turn off those banners.
Custom Applications	Test your custom apps, audit their design and implementation, keep up to date with newest web hacks – use OWASP
Firewalls	Many of the sources of those leaks can be screened at the firewall. Having a firewall isn't an excuse for not patching holes directly on the machine in question, but it goes a long way toward reducing the risk of exploitation.

Part II: Endpoint & Server Hacking

---

4. Hacking Windows

Unauthenticated Attacks:

- **Authentication spoofing**: The primary gatekeeper of access to Windows systems is the frail password. Common brute-force/dictionary password guessing and man-in-the-middle authentication spoofing remain real threats to Windows networks.
- **Network services**: Modern tools make it point-click-exploit easy to penetrate vulnerable services that listen on the network.
- **Client vulnerabilities**: Client software like Internet Explorer, Outlook, Office, Adobe Acrobat Reader, and others have all come under harsh scrutiny from attackers looking for direct access to end-user data.
- **Device drivers**: Ongoing research continues to expose new attack surfaces where the operating system parses raw data from devices like wireless network interfaces, USB memory sticks, and inserted media like CD-ROM disks.
  (Protect these avenues of entry to make your Windows system more secure.)

Spoofing Countermeasures:

- Use a network firewall to restrict access to potentially vulnerable services (such as SMB on TCP 139 and 445, MSRPC on TCP 135, and TS on TCP 3389).
- Use the host-resident Windows Firewall to restrict access to services.
- Disable unnecessary services (be especially wary of SMB on TCP 139 and 445).

- Enforce the use of strong passwords using policy.
- Set an account-lockout threshold and ensure that it applies to the built-in Administrator account.
- Log account logon failures and regularly review Event Logs.

Windows Authentication Sniffing Countermeasures:

- The key to disabling LM response attacks is to disable LM authentication. If you can prevent the LM response from crossing the wire, you will have blocked this attack vector entirely.
- For Kerberos attacks: use the PKINIT preauthentication method, which uses public keys rather than passwords and so does not succumb to eavesdropping attacks.
- For Kerberos: use the built-in Windows IPSec implementation to authenticate and encrypt traffic.

Man in the Middle (MITM) Countermeasures:

- Basic network communications and security fundamentals can help to protect against MITM attacks. The use of authenticated and encrypted communications can mitigate against rogue clients or servers inserting themselves into a legitimate communications stream.

Pass-the-hash Countermeasures:

- The pass-the-hash technique is inherent to the NTLM authentication protocol; all services using this authentication method (SMB, FTP, HTTP, etc.) are vulnerable to this attack.
- Using two-factor authentication might help.

Network Service Exploit Countermeasures:

- Test and apply the patch as soon as possible
- In the meantime, test and implement any available workarounds, such as blocking access to and/or disabling the vulnerable remote service.
- Enable logging and monitoring to identify vulnerable systems and potential attacks, and establish an incident response plan.

End-User Application Countermeasures:

- Deploy a firewall, ideally one that can also manage outbound connection attempts.
- Keep up to date on all relevant software security patches.
- Run antivirus (AV) software that automatically scans your system and keeps itself updated.
- Run with least privilege.
- Administrators of large networks of Windows systems should deploy the preceding technologies at key network choke points (that is, network-based firewalls in addition to host-based firewalls, antivirus on mail server, and so on) to protect large numbers of users more efficiently.
- Read e-mail in plain text.
- Configure office productivity programs as securely as possible.
- Don’t be gullible. Approach browsing with high skepticism. Don’t click links in emails from untrusted sources!
- Keep your computing devices physically secure.

Driver Exploit Countermeasures:

- Apply vendor patches ASAP.
- Disable the affected functionality (device) in high-risk environments.

Preventing Privilege Escalation:

- Maintain appropriate patch levels for Windows systems.

Pwdump Countermeasures:

- If DLL injection still works on Windows, there is no defense against pwdump derivatives. Administrator-equivalent privileges are needed to execute this.

Password Cracking Countermeasures:

- Can't contain the user's account name or parts of the user's full name that exceed two consecutive characters.
- Must be at least eight characters in length
- Must contain characters from three of the following four categories:
    - English uppercase characters (A – Z)
    - English lowercase characters (A – Z)
    - Base 10 digits (0 – 9)
    - Nonalphabetic characters (i.e. #, $, %, ^, &)

Password Cache Dumping Countermeasures:

- The best defense against lsadump2 and similar cache-dumping tools is to avoid getting Admin-ed in the first place. By enforcing sensible policies about who gains admin access to systems in your organization, you can rest easier.

Dumping Hashes Stored in Memory Countermeasures:

- Keep ALL security members of the Windows domain up to date.

Alternate Data Streams (ADS) Countermeasure:

- One tool for ferreting out NTFS file streams in Foundstone's sfind, which is part of the Forensic Toolkit v2.0 available at www.foundstone.com.

Windows Hardening Overview:

- The Center for Internet Security (CIS) offers free Microsoft security configuration benchmarks and scoring tools for download – www.cisecurity.org.
- Keep up to date with new Microsoft security tools and best practices available at www.microsoft.com/security.
- Don't forget exposures from other installed Microsoft products within your environment; for example, see www.sqlsecurity.com for great info on SQL vulnerabilities.
- Remember that applications are often far more vulnerable than the OS – especially modern, stateless, web-based apps.
- Minimalism = higher security. If nothing exists to attack, attackers have no way getting in. Disable all unnecessary services by using services.msc. For those services that are necessary, configure them securely (for example, disable unused ISAPI extension in IIS).
- If file and print services are not necessary, disable SMB.
- Use the Windows Firewall to block access to any other listening ports except the bare minimum needed for function.

- Protect Internet-facing servers with network firewalls or routers.
- Keep up to date with all recent service packs and security patches.
- Limit interactive logon privileges to stop privilege-escalation attacks before they even get started.
- Use Group Policy (gpedit.msc) to help create and distribute secure configurations throughout your Windows environment.
- Enforce a strong policy of physical security to protect against offline attacks

.

5. Hacking UNIX

UNIX is a complex system that requires much thought to implement adequate security measures. The sheer power and elegance that make UNIX so popular are also its greatest security weaknesses. Myriad remote and local exploitation techniques may allow attackers to subvert the security of even the most hardened UNIX systems. Buffer overflow conditions are discovered daily. Insecure coding practices abound, whereas adequate tools to monitor such nefarious activities are outdated in a matter of weeks. The table below contains some tools that can help:

Name	Operating System	Location	Description
Solaris 10 Security	Solaris	www.Nsa.gov/ia/_files/os/sunsol_10/s10-cis-appendix-v1.1.pdf	Highlights the various security features available in Solaris 10
Practical Solaris Security	Solaris	www.opensolaris.org/os/community/security/files/nsa-rebl-solaris.pdf	A guide to help lock down Solaris
Solaris Security Toolkit	Solaris	www.docs.oracle.com/cd/E19056-01/sec.tk42/819-1402-10/819-1402-10.pdf	A collection of programs to help secure and audit Solaris
AIX Security Redbook	AIX	www.redbooks.ibm.com/redbooks/pdfs/sg247430.pdf	Extensive resource for securing AIX systems
OpenBSD Security	OpenBSD	www.openbsd.org/security.html	OpenBSD security features and advisories
Security-Enhanced Linux	Linux	www.nsa.gov/research/selinux/	Enhanced Linux security architecture developed by NSA
CERT UNIX Configuration Guidelines	General	www.cert.org/tech_tips/unix_configuration_guidelines.html	A handy UNIX security checklist
SANS Top 25 Vulnerabilities	General	www.sans.org/top25	A list of the most commonly exploited vulnerable services
"Secure Programming for Linux and Unix HOWTO," by David A. Wheeler	General	www.dwheeler.com/secure-programs	Tips on security design principles, programming methods, and testing

6. Cybercrime & Advanced Persistent Threats

What is an APT?

- Advanced Persistent Threat was created by analysts in the US Air Force in 2006. It described three aspects of attackers that represent their profile, intent, and structure:
    - **Advanced**: The attacker is fluent with cyber-intrusion methods and administrative techniques and is capable of crafting custom exploits and tools.
    - **Persistent**: The attacker has a long-term objective and works to achieve his or her goals without detection.
    - **Threat**: The attacker is organized, funded, motivated, and has ubiquitous opportunity.

APTs involve multiple phases that leave artifacts:

1. **Targeting**: attackers collect info about the target from public or private sources and test methods that may help permit access. This may include vulnerability scanning (such as APPSEC testing and DDoS attacks), social engineering, and spear-phishing. The target may be specific or may be an affiliate/partner that can provide collateral access through business networks.
2. **Access/Compromise**: Attackers gain access and determine the most efficient or effective methods of exploiting the information systems and security posture of the target organization. This includes ascertaining the compromised host's identifying data (IP address, DNS, enumerated NetBIOS shares, DNS/DHCP server addresses, O/S, etc.) as well as collecting credentials or profile information where possible to facilitate additional compromises. Attackers may attempt to obfuscate their intentions by installing rogue ware or another malware.
3. **Reconnaissance**: Attackers enumerate network shares, discover the network architecture, name service, domain controllers, and test service and administrative rights to access other systems and applications. They may attempt to compromise Active Directory accounts or local administrative accounts with shared domain privileges. Attackers often attempt to hide activities by turning off AV and system logging (which can be a useful indicator of compromise).
4. **Lateral Movement**: Once attackers have determined methods of traversing systems with suitable credentials and have identified targets (of opportunity or intent), they will conduct lateral movement through the network to other hosts. This activity often does not involve the use of malware or tools other than those already supplied by the compromised host operating systems such as command shells, NetBIOS commands, Windows Terminal Services, VNC, or other similar tools utilized by network administrators.
5. **Data Collection & Exfiltration**: Attackers are after information, whether for further targeting, maintenance, or data that serves their other purposes – accessing and stealing information. Attackers often establish collection points and exfiltrate the data via proxied network cut-outs, or utilize custom encryption techniques (and malware) to obfuscate the data files and related exfiltration communications. In many cases, attackers have utilized existing backup software or other administrative tools used by the compromised organization's own network and systems admins. The exfiltration of data

may be “drip fed” or “fire hosed” out, the technique depending on the attackers’ perception of the organization’s ability to recognize the data loss or the attackers’ need to exfiltrate the data quickly.

6. **Administration & Maintenance:** Another goal of an APT is to maintain access over time. This requires administration and maintenance of tools (malware and potentially unwanted/useful programs such as SysInternals) and credentials. Attackers will establish multiple methods of accessing the network of compromised hosts remotely and build flags or triggers to alert them of changes to their compromised architecture, so they can perform maintenance actions (such as new targeting or compromises, or “red herring” malware attacks to distract the organization’s staff). Attackers usually attempt to advance their access methods to most closely reflect standard user profiles, rather than continuing to rely upon select tools or malware.

Indicators of a Compromise:

Malware, whether used by APTs or in “normal” situations, wants to survive a reboot. To do this, the malware can use several mechanisms, including:

- Using various “Run” registry keys
- Creating a service
- Hooking into an existing service
- Using a scheduled task
- Disguising communications as valid traffic
- Overwriting the master boot record
- Overwriting the system’s BIOS

When investigating, or conducting forensics, utilize proper order of volatility:

- Memory
- Page or swap file
- Running process information
- Network data such as listening port or existing connections to other systems
- System registry (if applicable)
- System or application logs
- Forensic image of disk(s)
- Backup media

When investigating, or conducting forensics, utilize a proper kit of tools. Examples include:

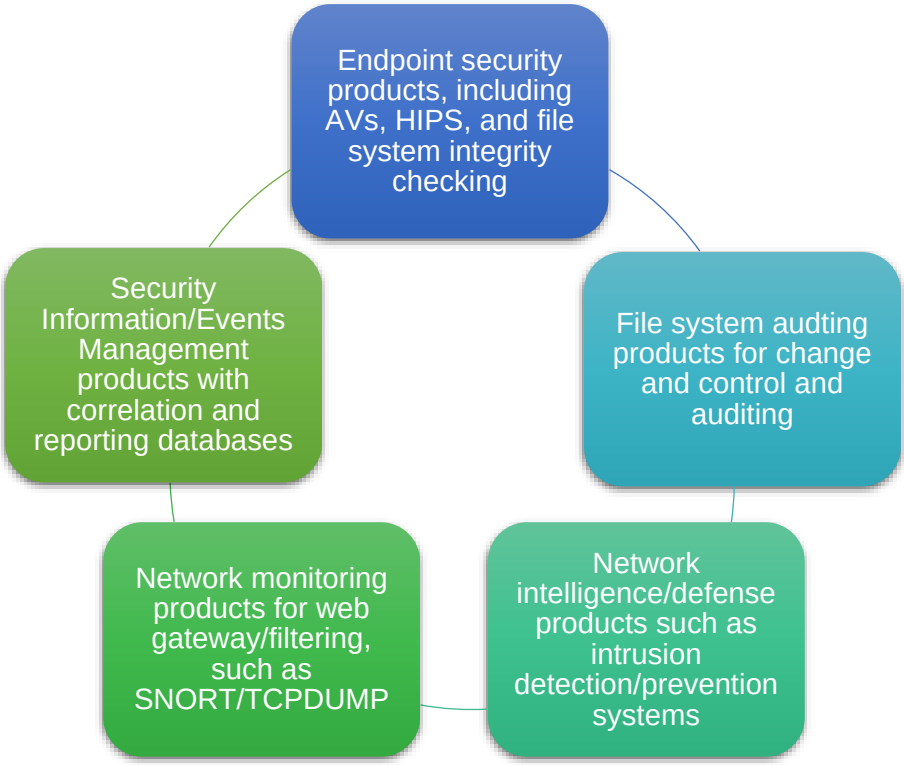
- AccessData FTK Imager
- Sysinternals Autoruns
- Sysinternals Process Explorer
- Sysinternals Process Monitor
- WinMerge
- Currports
- Sysinternals Vnmap

Common APT Indicators
✓ Networking communications utilizing SQL or private encryption methods, or sending and receiving base64-encoded strings

✓ Services registered to Windows NETSVCS keys and corresponding to files in the %SYSTEM% folder with DLL or EXE extensions and similar filenames as valid Windows files
✓ Copies of CMD.EXE as SVCHOST.EXE or other filenames in the %TEMP% folder
✓ LNK files referencing executable files that no longer exist
✓ RDP files referencing external IP addresses
✓ Windows Security Event Log entries of Types 3, 8, and 10 logons with external IP addresses or computer names that do not match organizational naming conventions
✓ Windows Application Event Log entries of antivirus and firewall stop and restart
✓ Web server error and HTTP log entries of services starting / stopping, administrative or local host logons, file transfers, and connection patterns with select addresses
✓ Antivirus/system logs of C:/ , C:/TEMP, or other protected areas of attempted file creations
✓ PWS, Generic Downloader, or Generic Dropper antivirus detections
✓ Anomalous .bash_history, /var/logs, and service configuration entries
✓ Inconsistent file system timestamps for operating system binaries

APT Detection:

Key detection technologies can help identify and combat these types of attacks, including the following:



Summary:

APT is the most dangerous type of cyber threat today. APTs provide ongoing access to protected institutional information. Such quiet yet dangerous intrusions are not limited in their scope. They can affect any company, government body, or nation, regardless of sector or geography.

Part III: Infrastructure Hacking

---

7. Remote Connectivity & VOIP Hacking

Dial-up & PBX Security Measures
1. Inventory existing in dial-up lines. Note unauthorized dial=up connectivity and snuff it out by whatever means possible. Additionally, consult whoever is responsible for paying the phone bill; this could give you an idea of your footprint.
2. Consolidate all dial-up connectivity to a central modem bank, position the central bank as an untrusted connection off the internal network (that is, a DMZ), and use IDS and a firewall to limit and monitor connections to trusted subnets.
3. Make analog lines harder to find. Don't put them in the same range as the corporate numbers, and don't give out the phone numbers on the InterNIC registration for your domain name. Password protect phone company account info.
4. Verify that telecommunications equipment closets are physically secure. Many companies keep phone lines in unlocked closets in publicly exposed areas.
5. Regularly monitor existing log features within your dial-up software. Look for failed login attempts, late-night activity, and unusual page patterns. Use Caller ID to store all incoming phone numbers.
6. **Important!** For lines that are serving a business purpose, do not disclose any identifying information such as company name, location, or industry. Additionally, ensure that the banner contains a warning about consent to monitoring and prosecution for unauthorized use. Have these statements reviewed by legal to be sure that the banner provides th3e maximum protection afforded by state, local, and federal laws.
7. Require multifactor authentication systems for all remote access. Multifactor authentication requires users to produce at least two pieces of information – usually something they have and something they know – to obtain access to the system.
8. Require dial-block authentication. Dial-block means that the remote access system is configured to hang up on any caller and then immediately connect to a predetermined number (where the original caller is presumably located). For better security, use a separate modem pool for the dial-back capability and deny inbound access to those modems (using the modem hardware or the phone system itself).
9. Ensure that the corporate help desk is aware of the sensitivity of giving out or resetting remote access credentials. All the preceding security measures can be negated by one eager new hire in the corporate support division.
10. Centralize the provisioning of dial-up connectivity – from faxes to voicemail systems – within one security-aware department in your organization.
11. Establish firm policies for the working of this central division, such that provisioning any new access requires extreme scrutiny. For those who can justify it, use the corporate communications switch to restrict inbound dialing on that line if all that is require is outbound faxing, etc. Get management buy-in on this policy, and make sure the have the

teeth to enforce it. Otherwise, go back to step 1 and show them how many holes a simple war dialing exercise will dig up.
12. Go back to step 1. Elegantly worded policies are great, but the only way to be sure that someone isn't circumventing them is to wardial on a regular basis. We recommend at least every six months for firms with 10,000 phone lines or more, but it wouldn't hurt to do it more often than that.

Brute-Force Voicemail Hacking Countermeasures:

- Deploy strong security measures on your voicemail system. Deploy a lockout on failed attempts. Log connections to the voicemail system and watch an unusual number of repeated attempts.

DISA Hacking Countermeasures:

- If you need DISA, work with the PBX vendor to ensure that DISA is configured with strong passwords and all default credentials are removed. Enforce a minimum of 6-digit authentication PINs, do not allow trivial PINs, and define a lockout for accounts of no more than 6 incorrect attempts.

VPNs:

Google Hacking for VPN Countermeasures:

- The best mechanism is user awareness. Those in charge of publishing web content should understand the risks associated with putting anything on the internet. Do annual checkups to search for sensitive information on their websites.

Probing IPSec VPN Countermeasures:

- You can't do much to prevent these attacks, especially when you're offering remote access IPSec VPN connectivity to users over the internet. Access control lists can be used to restrict access to VPN gateways providing site-to-site connectivity, but for client-to-site deployments, this is not feasible as clients often originate from various source IP addresses that constantly change.

IKE Aggressive Mode Countermeasures:

- The best countermeasure is to discontinue its use. Alternative mitigating controls include a token-based authentication scheme, which doesn't patch the issue but makes it impossible for an attacker to connect to the VPN after the key is cracked, as the key has changed by the time the attacker breaks it.

Citrix Hacking Countermeasures:

- Ask these questions:
    - Can you count the number of users on one hand?
    - Do you know them all by name?
    - Do you trust them implicitly with a shell on the inside of your network?
- If any of these questions is a NO, you must assess your Citrix environment.

VoIP Attacks:

SIP Scanning Countermeasures:

- Not much you can do against SIP scanning. Network segmentation between the VoIP network and the user access segments should be in place to prevent direct attacks

against SIP systems; however, once an attacker has access to this segment, they can scan it for SIP devices.

Pillaging TFTP Countermeasures:

- One method to help secure TFTP is to implement access restrictions at the network layer. By configuring the TFTP server to accept connections only from known static IP addresses assigned to VoIP phones, you can effectively control who can access the TFTP server and thus help mitigate the risk of this attack. Some controls to consider are:
    - Disable access to the settings menu on the devices.
    - Disable the web server on IP phones.
    - Use signed configuration files to prevent configuration manipulation.

VoIP Enumeration Countermeasures:

- Until all software developers settle on a proper way to deal with unexpected requests, SIP enumeration techniques will always be around. Security engineers and architects must constantly promote “defense in depth” by segmenting VoIP and user networks and by placing IDS/IPS systems in strategic areas to detect and prevent these attacks.

Remote Access Security SUMMARY:

- Password policy. Considering requiring two-factor authentication, such as smartcards or hardware tokens, before granting access from outside your network.
- Develop a policy for provisioning any type of remote access within your organization and audit compliance regularly with war dialing and other assessments.
- Find and eliminate unsanctioned use of remote control software (such as PCAnywhere) throughout the organization. The use of PCAnywhere should be reevaluated particularly due to the theft of its source code, which gives the attackers the ability to find bugs in the application that they may not have found without it.
- Be aware that modems aren’t the only thing that hackers can exploit over POTS lines – PBXes, fax servers, voicemail systems, and the like, can be abused to the tune of millions of dollars in long-distance charges and other losses.
- Educate support personnel and end users alike to the extreme sensitivity of remote access credentials so they are not vulnerable to social-engineering attacks. Remote callers to the help desk should be required to provide some other form of identification, such as personnel number, to receive any support for remote access issues.
- For all their glitter, VPNs appear vulnerable to many of the same flaws and frailties that have existed in other “secure” technologies over the years. Be extremely skeptical of vendor security claims and develop a strict use policy and audit compliance.

---

8. Wireless Hacking

Wireless gateways and multilayered encryption schemas have proved to be the best defenses for the plethora of tools currently floating around the Internet for attacking 802.11 WLANs. Ironically, wireless tech appears to be vastly different from other communication mediums; however, the industry model for layering security via multiple authentication and encryption schemas holds true. Here is a selection of excellent Internet-based resources if you choose to do more research into wireless tech:

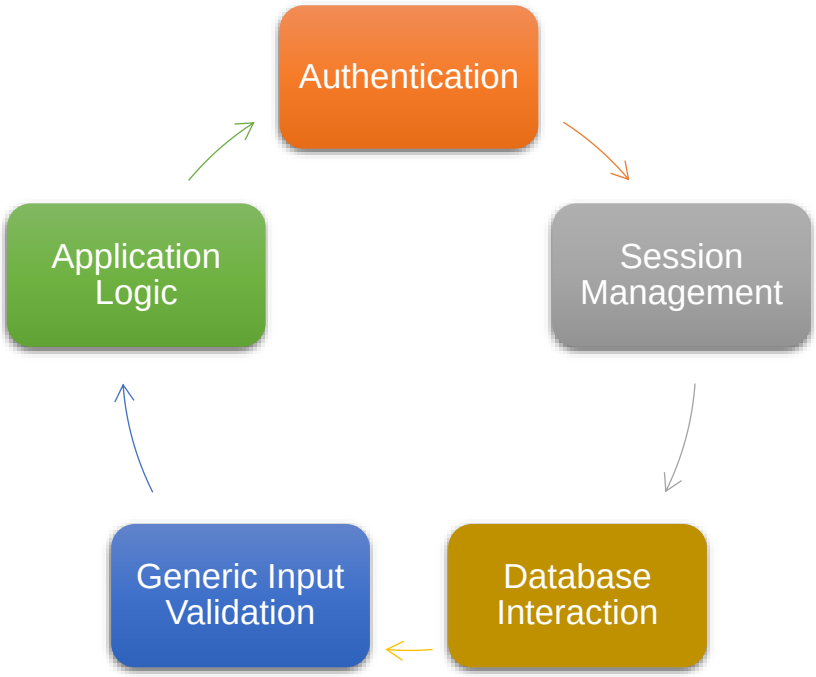
- www.standards.ieee.org/getieee802 : The IEEE designs and publishes the standard for 802.11 wireless transceivers, band usage (in cooperation with the FCC), and general protocol specifications.
- www.bwrc.eecs.berkeley.edu : The Berkeley Wireless Research Center (BWRC) is an excellent source for additional information on future communication devices and wireless technologies, especially those devices with high-integrated CMOS implementations and low-power consumption.
- www.l-com.com : L-com distributes wireless equipment from a wide variety of manufacturers, in addition to its own line of 2.4-GHz amplifiers that can be used for long-range transmitting or cracking.
- www.drizzle.com/~aboda/IEEE : The unofficial 802.11 Security Web Page has links to most of the 802.11 security papers as well as many general 802.11 links.
- www.airfart.sourceforge.net/ : Airfart is an excellent tool for viewing and analyzing, in real time, wireless access points and wireless card packets.
- www.hpl.hp.com/personal/Jean_Thourrilhes/Linux/Tools.html : Hewlett-Packard sponsors this page full of Linux wireless tools and research reports. It is an excellent source for all things Linux.
- www.wifi-plus.com : WiFi-Plus specializes in high-end antenna designs and sales, with a collection of antennas with ranged exceeding half a mile.

Part IV: Application & Data Hacking

---

9. Web & Database Hacking

Typical Web Application Attack/Analysis Framework:



Tools to use for web application analysis:

- Cookie Cruncher
- Encoders/decoders
- HTTP Editor
- Regular Expressions Editor
- Server Analyzer
- SOAP Editor
- SQL Injector
- Web Brute
- Web Discovery
- Web Form Editor
- Web Macro Editor
- Web Macro Recorder
- Web Fuzzer
- Web Proxy

Cross-Site Scripting (XSS) Countermeasures:

- Filter out input parameters for special characters – no web application should accept the following characters within input if possible: < > (?) # & “.
- HTML – encode output so even if special characters are input, they appear harmless to subsequent users of the application. Alternatively, you can simply filter special characters in output (achieving “defense in depth”).
- If your application sets cookies, use Microsoft’s HttpOnly cookies. This can be set in the HTTP response header. It marks cookies as “HttpOnly,” thus preventing them from being accessed by scripts.
- Analyze your apps for XSS vulnerabilities on a regular basis using the many tools and techniques for web apps analysis.

SQL Injection Countermeasures:

- Use bind variables (parameterized queries)
- Perform strict input validation on any input from the client.
- Implement default error handling
- Lock down ODBC
- Lock down the database server configuration
- Use programmatic frameworks

Cross-Site Request Forgery Countermeasures:

- The key to preventing CSRF vulnerabilities is somehow tying the incoming request to the authenticated session. What makes CSRF vulnerabilities so dangerous is the attacker doesn’t need to know anything about the victim to carry out the attack. Once the attacker has crafted the dangerous request, it works on any victim that has authenticated to the website. To foil this, your web application should insert random values, tied to the specified user’s session, into the forms it generates.

HTTP Response Splitting Countermeasures:

- The core countermeasure is solid input validation on server input.
- Consider performing output validation.

Hidden Tag Countermeasures:

- Limit the use of hidden tags to store information such as price – or at least confirm the value before processing it.

SSI Countermeasures:

- Use a preparser script to read in any HTML file, and strip out any unauthorized SSI line before passing it on to the server. Unless your app requires it, disable server-side includes and similar functionality in your web server's configuration.

Database Discovery Countermeasures:

- Never expose your databases directly to the internet.
- Segment your internal network and separate databases from other network segments by using firewalls and configuration options such as a valid-node checking for Oracle. Allow only a select subset of internal IP addresses to access the database.
- Run intrusion detection tools to identify network port scanning attempts.

DB Vulnerabilities & Countermeasures:

- **Network Attacks:**
  - Segment and use layered defense.
  - Apply DBMS vendor patches as soon as they are made available.
- **Database Engine Bugs:**
  - Apply DBMS vendor patches as soon as they are made available.
  - Monitor database logs for errors and audit user activity.
- **Vulnerable built-in stored objects:**
  - Apply Patches
  - Follow the least privilege principle, make sure to revoke access to dangerous database objects.
- **Weak or Default Passwords:**
  - Periodically scan DBs to discover and alert users to weak and default passwords.
  - Monitor application accounts for suspicious activity not originating from the application servers.
- **Misconfigurations:**
  - Create standards for each database platform and periodically scan your database to discover and alert on any deviations from the standards.
- **Indirect Attacks:**
  - Monitor and alert on suspicious privileged user's behavior.
  - Restrict what can run on the DBA system to known good programs only.
  - Do not click untrusted/unknown links in your web browser from your DBA system.
  - Strictly control user access to the DBA system.
- **There is no service pack for custom code:**
  - Regularly audit your own web apps

---

10. General Network Defense Strategy

Separation of Duties:

The premise behind this strategy is to separate the operational aspects of the countermeasure so the attacker must defeat multiple parallel factors. These are a few wars to achieve this:

Prevent, Detect, Respond: Utilizing at least two (ideally all three) of these types of countermeasures in parallel has been considered a fundamental of information assurance for many years:

- ✓ **Preventive**: endpoint hardening such as host intrusion protection systems (HIPS) software or network intrusion prevention
- ✓ **Detective**: network intrusion detection
- ✓ **Reactive**: incident response process execution

Checks & Balances: The classis separation of duties relates to the use of different accountable personnel to perform a given task. This classic method of protection can be beneficial and significantly reduce risk by:

- ✓ **Preventing collusion**: For example, if the detection personnel colluded with the reaction personnel, no one would ever know an incident had occurred.
- ✓ **Providing checks and balances**: for example, using a firewall rule to prevent access to a known vulnerable service.

Layering:

- ✓ **Physical:** physically secure servers in an access-controlled and monitored data center facility.
- ✓ **Network:** Use firewalls or other network device access control list (ACL) mechanisms to limit communications to only allowed service endpoints on specific hosts.
- ✓ **Host:** Utilize vulnerability management to keep service endpoint software up-to-date and utilize host-level firewalls and antimalware.
- ✓ **Application:** Patch off-the-shelf components and identify and fix bugs in custom components. Application firewalls.
- ✓ **Logical:** Control access (authentication and authorization) to the application's capabilities and data.

Passwords:

- ✓ Ensure all users have a password that conforms to organizational policy.
- ✓ Force a password change every 30 days for privileged accounts and every 60-90 days for normal users.
- ✓ Implement a minimum password length of eight characters consisting of one alpha character, one numeric character, and one alphanumeric character.
- ✓ Disable services that are not used.
- ✓ Implement password composition tools that prohibit the user from choosing a poor password.
- ✓ Don't use the same password for every system you log into.
- ✓ Don't write down your password.
- ✓ Don't tell your password to others.
- ✓ Use one-time passwords when possible.
- ✓ Don't use passwords at all. Use public key authentication
- ✓ Ensure that default accounts such as "setup" and "admin" do not have default passwords.

Security Patching:

- ✓ Test and apply the patch as soon as possible.
- ✓ In the meantime, test and implement any available workarounds, such as blocking access to and/or disabling the vulnerable remote service.
- ✓ Enable logging and monitoring to identify vulnerable systems and potential attacks, and establish an incident response plan.

General Strategy:

- ✓ There is no such thing as 100% countermeasure effectiveness. The only way to ensure 100% security is to restrict usability 100%, which is not viable. Achieving the right balance between these opposing goals is key.
- ✓ One of the key mechanisms to mitigate risk is diversification. By developing multiple, diverse obstacles, the attacker must invest more and differently at each point, raising the overall cost of successful attack more dramatically than with one (or many of the same types of) countermeasure.
- ✓ “Keep it simple stupid”: attackers go after the low-hanging fruit and frequently move on to easier targets when they don’t find it. Identify the obvious problems in your environment, create simple plans to address them, and sleep better at night knowing you’ve done your due diligence, based on empirical studies like the Verizon Data Breach Report.