

Router Security v2.0



**Linksys Malware 'The Moon'
Spreading from Router to Router**
LINKSYS®

**Real-World CSRF attack hijacks DNS
Server configuration of TP-Link routers**
TP-LINK®

**BT Home Flub: Pwnin
the BT Home Hub**



**ASUS Wireless router leaves USB Storage
Devices vulnerable to remote attackers**



**Control panel backdoor found
in D-Link home routers**



**Backdoor in wireless DSL routers lets
attacker reset router, get admin**
LINKSYS® NETGEAR

**Serious Vulnerabilities Found in
Popular Home Wireless Routers**
LINKSYS®

**Backdoor found in Chinese Tenda Wireless
Routers, allows Root access to Hackers**
Tenda®

**Actiontec MI424WR-GEN3I Router
Input Validation Hole Permits
Cross-Site Request Forgery Attacks**
Actiontec

AUGUST 13, 2016

ABHISHEK GAUTAM

What is a Router?

Routers are one of the **most important devices in a network**. Router plugs into a modem (and thus the Internet) on one end, and into all your computers on the other end. More specifically, a router talks to any and all computing device like **tablet, smartphone, desktop computer, laptop, Chromebook, thermostat, Apple TV, Smartwatch, Roku etc**, through either a **wired connection** (via Ethernet cables) or **wirelessly** (via Wi-Fi). The router is regarded as the source of the Wi-Fi network. Higher end routers can **create multiple Wi-Fi networks**, such as a one for **Private Network** and one for **Guests Network**. A router can be compromised in many ways by an attacker. Their main aim is taking routing decision to forward a packet to its destination. It can be a home or small office router which takes your traffic on the internet or it can also be one of the **CORE ROUTERS** (backbone of the internet). Being such an important component, routers are often targeted for attacks

The router hardware

Its roughly the **size of paperback book**.

It **may or may not have Wi-Fi antennas**.

Routers without visible antennas have internal ones.

There are routers with **one, two, three and four external antennas**.

Some routers announced at CES in January 2015 have **six or eight** antennas.

On some routers, the **antennas are removable, on others they are not**.

Wireless Wi-Fi networks can use two different range of frequencies, referred to as "**bands**".

- 1) The Older frequency band is **2.4GHz**.

- 2) The Newer one is **5GHz**.

Old or low end routers can only transmit in the 2.4GHz band. Many current routers transmit in both frequency bands at the same time, a condition known as **DUAL BAND**. A few routers (such as the Pepwave Surf SOHO) can **transmit in both 2.4GHz and 5GHz** but only one band at a time. High end routers support two separate 5GHz radios along with 2.4GHz. The term for this is **Tri-Band**(three concurrent frequency bands).

Flavours of Wi-Fi

- 1) “a” and “b” are the oldest.
- 2) Then came G(only 2.4Ghz).
- 3) Then came N(both 2.4GHZ and 5GHz)
- 4) Then came AC it works only on 5 GHz.

The 2.4GHz has better penetration through walls so it has longer range.

How routers vary?

These are the properties by which the ROUTERS vary amongst them:

- 1>There are **private and guest networks**. Guest networks are a great security feature, they can use a different password and be isolated from the private network. They can also be disabled when not needed.
- 2>The **number of networks vary**. A dual band router will, at the least, create one wireless network on each frequency band. They may also offer a guest network on each frequency band, for a total of 4 networks.
- 3>The **names vary**. While most routers let you chose any name you want for guest networks but some routers force you to use their name.
- 4> The **numbers of bands** they support and which **frequency** they can work on. For example: the routers can be single band, dual band, tri band and they may work at 2.4GHz or 5GHz or both.

Most routers do not have an **on/off switch**. Many of those that do position such that its just as easy to pull the electric plug as it is to hit the button. Almost all have lots of pretty blinking lights, but the number of lights and what they indicate vary greatly. Some routers let you **disable the blinking lights**. As a rule, routers **do not have microphones or speakers**. One exception is the **Starry Station** router which has both. The Google OnHub routers(Which google uses) have speakers, but no microphones.

Input to a router

Some routers have a **single WAN port**. Higher end routers have **multiple WAN ports** which allows them to be **connected to two or more different ISPs**. For example, one WAN port could be plugged into a cable modem and another into a DSL modem. This is for locations where Internet access is very important. The devices connected to the router to remain on-line even if one ISP fails.

Not all multi-WAN routers are the same. For example, there are **smart and dumb models**. The dumb ones **use ISP1 all the time, until it fails, and then switch over to ISP2**. Smart multi-WAN routers **use both ISP1 and ISP2 all the time and balance the load/traffic between them**. The smart ones can also tolerate the failure of a single ISP without anything connected to the router being aware of the problem.

There are also three different ways to feed the Internet into a router.

1. The most popular is **Ethernet**. Whether an ISP uses cable, DSL, satellite or fibre, its modem should be able to feed into any router via Ethernet.
2. Some routers, such as models by Pep link and Cradlepoint, can be fed by a **3G/4G/LTE modem plugged into a USB port**.
3. Finally, **Wi-Fi as input**. That is, if you are in a hotel that only offers Wi-Fi, you can feed that Wi-Fi into a router which then produces both Ethernet LAN as output and Wi-Fi as output.

Talking to a router



There are **MANY** ways to talk to a router after all it is a computer. The communication medium can be **wired Ethernet, wireless Wi-Fi, and/or Bluetooth**. Some high end models have a serial console port.

Figure 1 Internal Circuit of a Router

The most common way to interact with a router is via its **web interface**. That is, we communicate with a website that exists inside the router. Mostly this is done via the routers internal IP address. That is, you make a request such as

`http://192.168.1.1`

Each router can have a different interface and can have different functionalities implemented in That interface.



Figure 2 Router web interface example

After the web interface came the **cloud**. Hardware manufacturers created websites that could talk to and control your router. You need to register with the manufacturer website and get a userid/password. Then, you can **talk to your router from anywhere in the world**.

Some routers have **touch screen interface**. No doubt, **smartphone apps** are the wave of the future when it comes to communicating with a router. As noted above, Google exclusively uses a smartphone app to communicate with its router. the aforementioned Netgear Genie software, also runs on iOS and Android. Nerds may **talk to a router using SSH or Telnet**. Monitoring software may talk to it **using SNMP**. Some software communicates using **UPnP**.

New Router Initial Setup

Every set of instructions, I have seen from a router manufacturer says to **start the new router setup by plugging the router into the Internet**.

I disagree!!!

While a new router needs to be online to **get bug fixes (a.k.a. updated firmware)** I would first make the changes below while off-line

- Change the **default router password**
- Change the **default Wi-Fi password(s)**
- Change the **default Wi-Fi network name(s)**
- **Turn off WPS**

It is safer to plug it into a LAN port on an existing router. This puts a firewall in front of the new router, yet still lets it download updated firmware.

NOTE the operating system in the router is referred to as firmware.

This plan has one potential problem however: **IP address conflicts**: If the existing router is, for example, 192.168.1.1 and the new router also defaults to the same IP address, bad things will happen if the new router is plugged into the old one. The easy solution is put the new router directly on the Internet. **The better solution is to change the default IP address of the new router, something that should be done anyway.**

Changing Default IP Address of New Routers

One of the **first things to change** on a new router is the IP range it uses. That is, change the IP address of the router and the IP addresses given out by the DHCP server in the router (see below). Most routers that I have used were smart enough to modify the DHCP server settings when the IP address of the router was changed.

The reason behind using this is to **avoid some types of Attacks**.

One example of this is a **bug in D-Link routers** that was reported in January 2015 ([DNS hijacking flaw affects D-Link DSL router, possibly other devices](#)). Quoting:

"A vulnerability found in a DSL router model from D-Link allows remote hackers to change its DNS (Domain Name System) settings and hijack users' traffic ... Attackers don't need to have access credentials for the affected devices in order to exploit the vulnerability, but do need to be able to reach their Web-based administration interfaces ... Rogue code loaded from a website can instruct a browser to send specially crafted HTTP requests to LAN IP addresses that are usually associated with routers."

The critical point being that **using the same LAN IP addresses that everyone else does, makes you more vulnerable to certain types of attacks.**

Here is an example of malicious JavaScript attacking modems and routers: [Owning Modems And Routers Silently](#)(for more details visit <http://www.gironsec.com/blog/2015/01/owning-modems-and-routers-silently/>) This type of attack requires the bad guys to guess the IP address of the victim device.

If you use a non-standard IP address, you are relatively safe!

Another reason to choose a subnet that is off the beaten path is for VPNs. If, someday in the future, you setup a site to site VPN, having each site use its own subnet is cleaner and easier.

Regardless of the subnet, everyone is in the **habit of assigning their router an IP address that ends with 1**. This is a custom, not a requirement. Don't do it. Specifically, **do not use 191.68.0.1, 191.68.1.1 or 191.68.2.1**. Better choices on these same three networks are: 191.68.0.5, 191.68.1.11 and 191.68.2.250.

Which subnet to use?

I would **avoid the 192.168.x.x** networks that other devices by default do. That means, avoid networks where the third number is 0 (used in DLink) 0, 1 (used by Netgear, tplink), 2 (Used By Alpha) 0, 1, 2, 3, 5 (used by Hawking), 10, 11, 19 (Anonabox), 50 (Peplink), 55 (Luma), 86 (used by Google OnHub router), 88 (used by MikroTik), 100 (cable modems) and 178 (FRITZBox). That is, avoid 192.168.0.x, 192.168.1.x and 192.168.100.x.. Some good networks would be 192.168.68.x or 192.168.77.x or 192.168.90.x.

If you like 10.something, then **avoid 10.0.0.x , 10.0.1.x, 10.1.1.x and 10.10.10.x** (used by HooToo in their HT-TM05 TripMate Titan Wi-Fi sharing device). Keep default IP such that something that no one would guess, like 10.43.27.x is better.

Other attacks that need to know (or guess) the internal IP address of the router:

- **A JavaScript based attack:** [Bruteforcing TP-Link routers with JavaScript](http://www.xexexe.cz/2015/02/bruteforcing-tp-link-router-with.html) (www.xexexe.cz/2015/02/bruteforcing-tp-link-router-with.html) Feb. 4, 2015. This attack can learn the LAN side IP address of the computer it is running on, so it assumes the router IP address ends with 1. It can be foiled by changing the router password.
- [CSRF, Backdoor, and Persistent XSS on ARRIS / Motorola Cable Modems](#) by Tod Beardsley of Rapid7 June 5, 2015. Although the headline uses the term "modem" the vulnerable device is a gateway (modem-router combination). Quoting: "The attacker must successfully know, or guess, the victim's internal gateway IP address".

TOR AND VPN CLIENT ROUTER

InvizBox(invizbox.io) is a Tor router based on **OpenWRT** released in March 2015 for \$39. The second generation, called InvizBox Go will do both VPN and TOR. Both models are open source. The Tiny Hardware Firewall was endorsed by Leo Laporte, a.k.a. The Tech Guy. There are three models, sold by the vendor for \$30 or \$35. The smallest model has no Ethernet ports (it's too small), the other two models have an Ethernet WAN port and an Ethernet LAN port. A *big* limitation is that it works with only one VPN provider, HotSpotVPN. Purchases come with one year of VPN service. Expect to pay about \$91 for the second year of service. Laporte warns that it can take 5 minutes to boot up. He also claims that it can engage both the VPN and TOR at the same time. These are low end devices, Ethernet is 100Mbps, Wi-Fi is G and N.

VPN Client Routers

When most consumers encounter a VPN router, they are dealing with a router that can function as a VPN server. the software necessary to connect to a VPN server, is built into the firmware. Very few routers, running the software they shipped with, can function as a VPN client. The most popular seem to be OpenVPN, L2TP/IPsec and PPTP with PPTP being the worst option as it is the least secure.

TOR Routers

- Onion Pi is a Raspberry Pi-based TOR router that sells for about \$70. You have to install TOR yourself.
- The Personal Onion Router to Assure Liberty (PORTAL) is a build it yourself TOR router. It is not a hardware product that you can buy, rather, it is software that needs to be installed on a limited number of supported routers.
- The PogoPlug Safeplug is also a TOR router. Consumer Reports liked it, but a more trustworthy source said the security it uses stinks.
- The Cloak router at <https://reclaim-your-privacy.com> will be a cheap router with two networks: one that is normal and one that sends all traffic through the TOR network. It will run a modified version of OpenWrt.



PENETRATION TEST



Router Penetration Testing

Router Pen testing is a process in which we try to identify all the possible information about the router firmware, settings, open ports, filtered ports, services, company manufacturer, ROM released date, Model Number, IP table capacity etc and perform attack on routers and make a report from the attacks we performed.

Three Kind of Penetration Testing to Generate Report for Client

1. Exploit misconfigured services (FTP, TELNET, SSH, WPS, etc)

> **Default passwords:** These passwords depends upon the model number and company of the router manufacturer. So we must have a standard list of all the popular routers with their default username and password which will land us to the dashboard area of any router.

For Example: We must have a dump of <http://www.routerpasswords.com/> list passwords and usernames whenever we are going to the client site.

> **Password Brute forcing:** Password brute forcing works only when CAPTCHA is not implemented in ROM of the router hence this permutation and combination attack can be done only without CAPTCHA authentication screen, this includes both dictionary based brute forcing and permutation combination based brute forcing.

For Example: Fireforce - Mozilla Plugin or Hydra Brute Forcer

2. **Exploiting known router vulnerabilities:** On daily basis there are many vulnerabilities and attacks which are getting launched in public domain on vulnerability databases online like exploit-db.com and packetstormsecurity.org. We have to identify the router model number and firmware to make sure if any public domain exploit is available to gain access in that router.

1. <http://192.168.0.1/DevInfo.txt>

2. DDOS Attack on Router

3. Attacking the web interface

- > Command injection
- > Source Code disclosure (.txt, .inc, .conf)
- > Directory transversal
- > CSRF
- > XSS

Basic Steps to Perform VAPT of Routers

Step 1: Information gathering

- > Get the IP address of the router
- > scan for open ports/services (nmap/zenmap)
- > Check the architecture of the web interface
- > get the model number and vendor of the router

Step 2: VA

- > Search for default passwords of the model
- > search for known vulnerabilities (exploitdb, cvedetails, google)
- > Use scanners like nessus

Step 3:PT

- > Try default passwords(admin:admin, admin:<blank>, admin:password, google passes)
- > Try brute forcing the services/web interface (medusa, hydra, patator)
- > run available exploits
- > Pickup the router and look for password underneath it
- > press the reset button on the router to reset it to default settings

Step 4: Gain Access

Step 5: Privilege escalation

- > Try gaining root access
- > Escalating into another network

Step 6: POST exploitation

- > Change DNS Entries for phishing
- > Cause Denial of Service
- > Steal Login Credentials of ISP
- > Get the Wi-Fi password

Step 7: Mantain Access

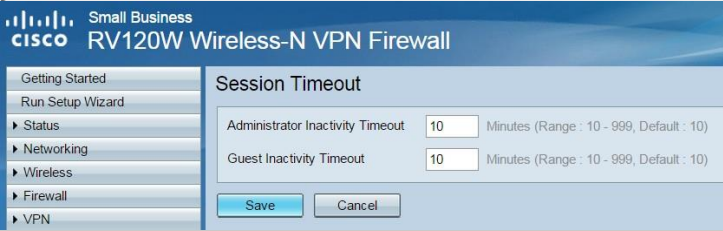

- > Upload Backdoor
- > disable Security settings
- > Allow login from external IPs

Step 8: Flush the logs

Security Checklist

The most expert person in the world can only make a router as secure as the firmware (router OS) allows. The following list of security features lets you judge how secure a router can potentially get. If you care to make your router more secure perform and check the following security checklist. Sadly, reviews of routers never discuss any of this.

| SNo. | Test | Description |
|------|---------------------------|---|
| 01 | PHYSICAL TEST | The routers should be placed such that physically they are not easily accessible as in that case someone might easily reset the router or sometimes on the back of router the username and passwords are written and that can be misused easily or can get connected with that router using a LAN cable (if one of four LAN ports are available). |
| 02 | WPS SUPPORT TEST | WPS has been such a security disaster . Since WPS is required for Wi-Fi certification, it is present in all consumer routers. Thus, it is best not to use a consumer router. If you are using a router that supports WPS, then check to see if it can be turned off . Some of the firmwares of routers don't allows to disable the wps option so do check that before buying any router. To check if wps is disabled or not use a Wi Fi survey type application such as the excellent Wi Fi Analyzer on Android. On Windows, look into Wi-FiInfoView from Nirsoft - it is free and portable. Apple doesn't allow any such app on IOS. |
| 03 | NO DEFAULT PASSWORDS TEST | Default passwords are a huge problem for routers and should not be allowed. Even default passwords that look random are not. Eventually, someone figures out the formula for creating that password and can often use that, combined with public information from the router, to derive the password. |
| 04 | LOCAL ADMINISTRATION TEST | A malicious person on your network is bad enough, but we need to prevent them from being able to modify the router, for this we need to have a local administrator which has all privileges. Check the following: >>Can admin access be limited to Ethernet only? >>Can the port used for the web interface be changed? >>Can access be restricted by LAN IP address? >>Can access be restricted by MAC address? >>Can router access be restricted by SSID? |
| 05 | CSRF | The router also needs to be protected from malicious web pages that exploit CSRF bugs. |
| 06 | HTTPS SUPPORTED | Some support HTTPS, some do not. Every router that support it. However, had it mostly disabled by default. |
| 07 | LOGON TEST | The router should not allow multiple computers to logon at the same time using the same userid. So at a time max one login. |

| | | |
|----|----------------------------------|--|
| 08 | CAPTCHA OPTION | Router should implement captcha login(D-LINK offers this on some router). |
| 09 | TIME OUT TEST | <p>you should be able to set the timeout period.eg:</p>  |
| 10 | LOGOUT FROM WEB INTERFACE | Router should implement this facility(some models of DLINK does not support logout). |
| 11 | REMOTE ADMINISTRATION | <p>It is an important feature which allows to remotely change and monitor router settings</p>  |
| 12 | WI-FI | <p>No one can hack into a network that does not exist.</p> <p>>>Can the wireless network(s) be scheduled to turn off at night and then back on in the morning? Is there a Wi-Fi on/off button? This seems to be a rare feature. Some routers with it are the TP-Link Archer C9 and D9, the Asus RT-AC68U, The Netgear R6220 and the Synology RT1900ac. The idea is to make it easier to disable Wi-Fi when it's not needed. When this is easily done, more people will do it.</p> |
| 13 | WPA2 | <p>Although every router offers WPA2 encryption with Pre-Shared Key (PSK) there are still things to look for:</p> <p>>>verify that the router offers WPA2 exclusively. If the only option is a combination of WPA and WPA2, then it is not as secure as WPA2.</p> <p>>>After opting for WPA2 encryption, a better router will always use AES or CCMP (two terms for the same thing). Some routers offer TKIP as an option with WPA2. TKIP is not as secure.</p> <p>Wi-Fi Analyzer on Android, to see if it is using AES, CCMP or TKIP.</p> |
| 14 | GUEST NETWORKS | <p>Guest networks are good but all guest networks are not same so please always do check these:</p> <p>Is the network defined normally or does it require a captive portal? Normal is good, captive portal is bad</p> |

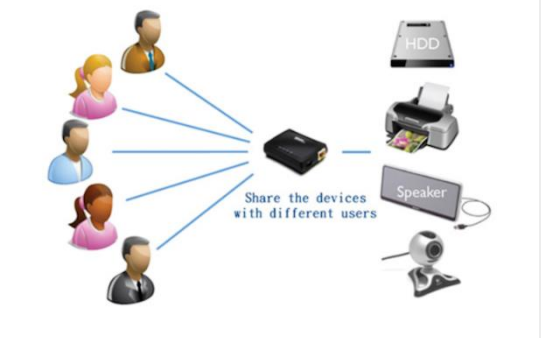
| | | |
|----|-------------------------------|---|
| | | <p>guest users should not be able to see anything that is Ethernet connected to the router, or, anything that is connected to a non-guest wireless network from the same router. One way to verify it is with a LAN scanner app such as Overlook Fing which runs on iOS, Android, Windows and OS X. The scan should not see any devices on the private network. Another option is, from a guest network, to try and access a NAS or a network printer or any other LAN device exposing a web interface. Some routers have a configuration option for guest users being able to see each other. It is more secure if they cannot, but there may be times where you want to allow this. Some routers combine isolation and disallow to see guests which is not a good option to combine.</p> <p>Some routers let you schedule the guest network(s). It would be great if you could turn it on for X hours and then have the router deactivate it. Probably the worst thing about guest networks is leaving them on <i>all</i> the time. Look for a limit on how long a guest user may be logged on to the guest network. The guest network should share a different subnet mask than private network. Nice to have: Some routers let you limit the bandwidth of guest networks.</p> |
| 15 | ROUTER USERID | <p>Every router lets you change the password, a few let you also change the userid. This is most important when using Remote Administration. Most routers only allow for one userid, but some allow for two: one with full admin privileges and one that is only allowed to view stuff but not make changes.</p> |
| 16 | ROUTER PASSWORD | <p>Test how long the password can be? Very short passwords should not be allowed. What chars and symbols are allowed in passwords and check if the password is strong enough?</p> |
| 17 | BRUTE FORCE PASSWORD GUESSING | <p>Test After a certain number of wrong passwords does the router do anything to prevent further guessing?</p> <p>Mitigation: This is solved by session locking.</p> |
| 18 | FIREWALL | <p>Kick the tires on the firewall looking for open ports</p> <p>All routers should get a perfect score at Steve Gibson's ShieldsUP!(@https://www.grc.com/shieldsup)</p> |

| | | |
|----|--------------------------------|--|
| | | Run both the Common Ports test and the All Service Ports test. If all is well, it will say "Passed" in green and the status of every port will be "stealth". The passing grade also means that the router does not reply to Ping commands on the WAN port. |
| 19 | MAC ADDRESS FILTERING | <p>The big question with MAC address filtering is whether this feature applies to all networks created by the router, or, to all networks on the same frequency band (2.4GHz or 5GHz), or, in the best case, if there are separate MAC filtering lists for <i>each</i> individual network/SSID? If a router supports independent filtering lists for <i>each</i> SSID, then MAC address filtering can be used for the main, private SSID and not used on guest networks. This makes it a practical solution as the maintenance hassle is so low.</p> <p>>>Another aspect that can make this much easier to deal with is comments. That is, instead of just maintaining a list of black- or white-listed MAC addresses, the router should also let you add a comment to each MAC address. This way you can easily check if computer X is already in the list or not. And, when tablet Y is lost, it makes it easy to remove it from the list.</p> |
| 20 | UPnP (UNIVERSAL PLUG AND PLAY) | <p>UPnP can be a security problem as it is used to poke a hole in the firewall. Most routers let you disable UPnP. Check if yours does and verify this using the two online testers below</p> <p>>>Does your router pass Steve Gibson's UPnP exposure test? This is the big orange button at <u>ShieldsUP!</u> It must.</p> <p>If you must use UPnP, then look for a router that offers detailed status information about the state of forwarded ports, such as the app that made the UPnP request and details on the currently active port forwarding rules. Some port forwarding rules come from UPnP and some don't. It is best to use a router that clearly shows which port forwarding rules came from UPnP requests.</p> <p>Eg TPLINK ARCHER C7</p> |
| 21 | PORT FORWARDING | Test Can it be limited by source IP address and/or source IP subnet? The secure answer is yes. The router should also schedule the port forwarding options. |
| 22 | IP SPOOF PROTECTION | >>Router should implement anti-spoofing using the access list. |

| | | |
|----|--------------------------------|--|
| | | <p>>>Drop communications from multicast addresses. A multicast address cannot be used as a source address, so such communications are not valid.</p> <p>Mitigations:</p> <ol style="list-style-type: none"> 1. Use authentication based on key exchange between the machines on your network. something like IPsec will significantly cut down on the risk of spoofing. 2. Use an access control list to deny private IP addresses on your downstream interface. 3. Implement filtering of both inbound and outbound traffic. 4. Configure your routers and switches if they support such configuration, to reject packets originating from outside your local network that claim to originate from within. 5. Enable encryption sessions on your router so that trusted hosts that are outside your network can securely communicate with your local hosts. |
| 23 | ARP SPOOF PROTECTION | <p>Mitigations:</p> <p>1)Dynamic ARP Inspection (DAI) is a security feature that is available on Cisco Catalyst 6500 Series switches running Cisco IOS Software or Cisco Catalyst OS. Dynamic ARP inspection helps prevent ARP poisoning and other ARP-based attacks by intercepting all ARP (Address Resolution Protocol) requests and responses, and by verifying their authenticity before updating the switch's local ARP cache or forwarding the packets to the intended destinations.</p> <p>2)Enable DHCP Snooping</p> |
| 24 | DNS SPOOFING PROTECTION | <p>Mitigations:</p> <p>Test if router implements following or not</p> <p>>> SOURCE PORT RANDOMISATION: Source port randomization makes it more difficult for the attacker to spoof DNS responses by randomizing the source UDP port used to send queries from the DNS server. With source port randomization the attacker must correctly guess both the transaction ID and the source port of the query.</p> |
| 25 | HNAP TEST | <p>This should always be disabled The Home Network Administration Protocol has been the basis for multiple router flaws. In April 2015 it was found</p> |

| | | |
|----|----------------------------------|---|
| | | to make a number of D-Link routers vulnerable. In Feb 2014 it was used as part of an attack on Linksys routers. |
| 26 | FIRMWARE | <p>Check Can you be passively notified (typically via email) by either the router or the company that produced it, when there is new firmware?</p> <p>For a new router: does it attempt to update the firmware as part of the initial setup process? Stats say 10 out of 20 routers don't do it.</p> <p>>>For an existing router: can it automatically update the firmware on its own?</p> <p>>>Assuming there is no automatic firmware update process, then the question becomes how easy is the upgrade process. Better routers can completely handle a firmware update in the web user interface. Lesser routers force you to download a file, then upload it back to the router. This harder procedure makes it less likely router owners will update the firmware.</p> <p>>>The new firmware may reset some options. To protect against this, it's a good idea to manually backup all the current settings before upgrading. If there is a function in the web interface to check for new firmware, does it actually work?</p> <p>>>Is the firmware downloaded securely? (HTTPS, SFTP or FTPS) There are two parts to this question as the firmware may be downloaded by the router itself or by you manually from the vendor's website.</p> <p>>>check Is the new firmware validated before it is installed?</p> <p>>>Does the router support multiple installed firmwares? This <i>great</i> feature lets you back out from a firmware update that causes problems and thus eliminates most of the risk that always exists when installing new software.</p> |
| 27 | Misfortune Cookie flaw | Is the router vulnerable to the <u>Misfortune Cookie</u> flaw? This is not something we can test for ourselves, nor is there a full list of vulnerable routers anywhere. We need to have the router manufacturer issue a statement. So this is really a test of how the router vendor handles security issues. Did they post anything on their website? If you ask them, will they intelligently respond? |
| 28 | BLOCKING ACCESS TO MODEMS | Check if it can block access to modems by ip address or not. |
| 29 | LOGON | Is there a log file (or files)? There should be, and hopefully, the data in the log is reasonably understandable and useful. |

| | | |
|----|------------------------------------|---|
| | | <p>Does it log unsolicited incoming connection attempts?</p> <p>Does it log failed logon attempts? Successful logons? Failed logons are obviously good to know about, but so too are successful logons, just in case the person in charge of the router was <i>not</i> the one who successfully logged in. Hopefully, the logged information includes the source IP address.</p> <p>Is anything logged when a new device joins the LAN? It would make a great audit trail if the router logged the client MAC address every time a new device joined the network.</p> <p>Can it log all Internet access by a single device?</p> <p>Does it log changes made to the router configuration?</p> <p>Do the log files disappear when the router is powered down?</p> |
| 30 | EMAIL | <p>Check Can the router send an email message when something bad happens?</p> <p>If so, what types of errors can it email about? At the least, it should be able to send an alert if one of the log files fills up.</p> <p>This is particularly useful for multi-WAN routers, that is, routers that are connected to two or more ISPs. When one Internet connection fails, it can use another to send an alert email.</p> <p>Can messages be sent to only one recipient or to many?</p> <p>*note*there are services that can convert these emails into text alert</p> |
| 31 | DDNS | <p>Not everyone needs DDNS, it is mostly used for remote administration. If you do need it, there are some options to look for.</p> <p>Does the router phone home to the DDNS provider using HTTP or HTTPS?</p> <p>How many DDNS providers are supported? The more the better.</p> |
| 32 | MONITORING ATTACHED DEVICES | <p>It's nice to know who/what is connected to the router A good router will offer, at a glance, a list of <i>all</i> the attached devices. Having them all shown on one screen makes it easy to spot anything out of the ordinary.</p> <p>>> Internet sessions/sockets: It can be very handy to see all the connections a LAN-resident device has to the Internet.</p> <p>>>Non-security: If the router is creating multiple Wi-Fi networks, it is nice to see which devices are connected to which network.</p> |

| | | | |
|----|---|---|--|
| 33 | netUSB | <p>Can you disable the file sharing of storage devices plugged into a USB port? This came up in May 2015 with the industry-wide NetUSB flaw. Some routers let you disable the buggy file sharing, others did not.</p> |  |
| 34 | Ssid Hiding | SSID hiding: Like MAC address filtering, this offers only a small increase in security and comes with a high hassle factor. | |
| 35 | SMARTPHONE APPS | <p>Does the app talk directly to the router or does it talk to the hardware vendor?</p> <p>Does the app communicate with Bluetooth or Wi-Fi?</p> <p>If app uses Wi-Fi, is it HTTP or HTTPS?</p> <p>If app uses Bluetooth, how secure is it?</p> | |
| 36 | VLAN's | Does the router implement the concept of virtual LAN's this is useful when if the attacker gains access to one part of the network then the other parts must be isolated from it | |
| 37 | ABILITY TO MODIFY THE ETHERNET MAC | ability to modify the Ethernet MAC address that is used as the base of Wi-Fi networks. This would allow a router of brand X to masquerade as brand Y. This is a common feature, but it mostly applies to the WAN port. It exists because some ISPs use the MAC address as part of their security. | |
| 38 | DNS SERVER TESTS | <p>A very common thing that bad guys do when they attack a router is change the DNS servers. There are many reasons for this, one is that almost no one will detect the change. A great defence is knowing what the DNS servers in a router <i>should</i> be.</p> <ul style="list-style-type: none"> • <u>DNS Leak Test</u>(@ www.dnsleaktest.com) is the best site for this that I have run across. It is well suited to non-techies. • <u>ipleak.net</u> is from VPN provider AirVPN. It reports lots of things, including DNS servers. It is only available via HTTP, not HTTPS. It is also available on ports 8000 and 62222. • The <u>F-Secure Router Checker</u> does not really check routers, but it does report . <p>One known bad DNS server is 91.194.254.105.</p> | |
| 39 | FIREWALL TESTERS | <p>To see what Shodan knows about your router, replace the X's in this link https://www.shodan.io/host/xxxxxx with your public</p> | |

| | | |
|----|--|---|
| | | <p>IP address. A result of "Not Found" is best. Among the many sites that report your public IP address are: ipchicken.com, checkip.dyndns.com and www.unix.com/what-is-my-ip.php</p> <p>>>Individual ports can also be tested with Telnet. To install the Telnet client on Windows 7 and 8: Control Panel -> Programs and Features -> click on Turn Windows features on or off in the left side column -> Turn on the checkbox for Telnet Client -> Click OK. To use telnet, open a Command Prompt window, type "telnet ip address port number". For example: telnet 192.168.1.1 80. If the port is closed, Windows will complain that it "could not open connection to the host on port 80: connect failed". If the port is open, the responses vary, you may just see a blank screen. You can also telnet to a computer by name, such as "telnet somewhere.com 8080"</p> |
| 40 | IP VERSION 6 TESTER | <ul style="list-style-type: none"> The only website that I know that tests for the existence of IPv6 is whatismyv6.com. After turning off IPv6 in the router, test it here. Click on the "IPv6 only Test" or go directly to ipv6.whatismyv6.com. |
| 41 | ANDROID APP TO CHECK FOR MISCONFIGURED SETTINGS | <p>According to the company, <u>Router Check</u> "is the first consumer tool for protecting your home router ... RouterCheck is like an anti-virus system for your router. It protects your router from hackers..." It's an <u>Android app</u> which can be used to check the misconfigured settings of your router.</p> |
| 42 | DHCP STARVATION ATTACK | <p>The router should be configured in such a way that this attack does not happen and to do so we need to enable the switch port security and the DHCP Scoping</p> <p>Mitigations:</p> <ol style="list-style-type: none"> 1)Switch port security 2)DHCP Scoping |
| 43 | PRIVILEGE ESCALATION | <p>We should always test that once by gaining access to a router can we also gain access to the root.</p> |
| 44 | UNUSED ROUTER INTERFACE DISABLED OR ENABLED | <p>Any unused router ports need to be disabled. If not disabled, you can easily shutdown unused interface using shutdown command.</p> |
| 45 | CHECKOUT SNAM CONFIGURATION | <p>SNAM configuration parameters such as SNMP need to be permitted for a certain class of IP address, default community strings (public, private) must be changed when the router comes online for the first time in network.</p> |

| | | |
|----|---|---|
| 46 | WHO RECEIVES SYSLOG | Make there is access-list in place to ensure that only administrators are able to receive the syslog and only their systems have access to the log host machine. |
| 47 | TFTP | Make sure TFTP is disabled, if not in use. |
| 48 | REDUNDANT ROUTER | Is there any redundant router-either hot or cold standby? |
| 49 | ACTION PLANS | What is the action plan if any malicious activity is noticed? |
| 50 | ROUTING RULES | <p>Is IP directed broadcast disabled on each router interface ('no ip directed broadcast')?</p> <p>B. Is source routing disabled on each router interface ('no ip source-route')?</p> <p>C. Is IP unreachable disabled on each router interface ('no ip unreachable')?</p> <p>D. Are inbound anti-spoof filters applied on external router interfaces?</p> <p>E. Are inbound ACLs defined to block RFC1918 - reserved and internal IP addresses on external router interfaces?</p> <p>F. Are outbound anti-spoof filters applied on external router interfaces?</p> <p>G. Are outbound traffic that does not have a valid internal source IP address blocked on external router interfaces?</p> <p>H. Are defined ACLs appropriate and as restrictive as possible (e.g. permitting specific IP addresses instead of IP address ranges, etc)?</p> <p>I. Are ACL entries ordered in terms of traffic volumes for efficient use of CPU cycles?</p> |
| 51 | SECURITY MANAGEMENT - ACCESS CONTROL | <p>Is the list of authorized users reviewed on a regular basis? Inactive accounts should be disabled and deleted in a timely manner.</p> <p>>> Are passwords encrypted in the router configuration (e.g. using 'enable secret', 'service password-encryption', etc)?</p> |
| 52 | AUDIT / LOGGING | <p>Are audit (e.g. syslog) functions enabled?</p> <p>B. Are logs of appropriate level (e.g. informational) recorded?</p> <p>C. Are Deny ACLs logged (Parameter 'log' or 'log-input' should be configured at the end of the ACLs to be logged)?</p> <p>D. Are log entries recorded on a secured management workstation and reviewed by the network group on a regular basis?</p> <p>E. Are system logs archived on a regular basis?</p> |
| 53 | DIRECTORY TRAVERSAL | Directory traversal is an HTTP exploit which allows attackers to access restricted directories and execute commands outside of the web server's root directory. With a system vulnerable to |

| | | |
|----|------------------------------------|---|
| | | directory traversal, an attacker can make use of this vulnerability to step out of the root directory and access other parts of the file system. This might give the attacker the ability to view restricted files, or even more dangerous, allowing the attacker to execute powerful commands on the web server which can lead to a full compromise of the system. |
| 54 | AUTHENTICATION BYPASS | It allows the attacker to perform some action that the application designer saw fit to restrict to authenticated users <i>without</i> providing said authentication. |
| 55 | Information Disclosure | If We are able to view (.txt,.inc,. conf) then such vulnerabilities exist. |
| 56 | Remote code execution | Remote code execution means we can execute code at router from our computer |
| 57 | Command injections | We can run command in the cmd of the router if this vulnerability exist |
| 58 | Protection from DoS attacks | ACL should be properly configured. |
| 59 | SYN Flood Protection | Applied Inbound on External Interface access-list 106 permit tcp any <Internal Subnet> established access-list 106 deny ip any any log |
| 60 | Land Attack Protection | Applied Inbound to External Interface access-list 100 deny ip host <External IP> host <External IP> log access-list 100 permit ip any |
| 61 | Smurf Attack Protection | Applied Inbound on External Interface access-list 110 deny ip any host x.x.x.255 log access-list 110 deny ip any host x.x.x.0 log x.x.x = Internal Subnet |
| 62 | Interface | Disable ability to spoof and perform probes no ip proxy arp no ip directed-broadcast no ip unreachable no ip mask-reply no ip redirects |
| 63 | NTP | <ul style="list-style-type: none"> Set clock configuration <ul style="list-style-type: none"> clock time zone UTC 0 no clock summer-time |

| | | |
|----|---|---|
| | | <ul style="list-style-type: none"> • Only allow NTP on Interfaces, using access list • Use Authenticated NTP |
| 64 | Stack based buffer overflow | It allows a remote attack to execute arbitrary code. A stack-based buffer overflow occurs in the function within the cgin binary which validates the session cookie. |
| 65 | Distributed Denial of Service Attack | <p>Distributed Denial of Service attack causes a victim to be denied of service that he requests. Here there are multiple hosts which perform this attack on system.</p> <p>They scan for vulnerable hosts and if vulnerable hosts are found then the tools are installed on them and these tools also scan for vulnerable application and installs itself on those systems also. This whole process happens very fast and repeatedly and then when there are enough users to make attack effective then attack is launched on the router. In stateful firewall solutions, there is a component commonly known as the stateful packet inspection (SPI) engine. This is also referred to as DPI (deep packet inspection). This engine provides intelligence by looking into the packet flow to determine and define connection information and application-level details</p> <p>IDS/IPS devices are often deployed at the network core and/or edge and provide intelligent decision capabilities by using DPI to analyze and mitigate an array of attacks and threats.</p> <p>Load balancers use SPI to make decisions based on the connections that traverse the load balancer function</p> <p>ROUTER FILTERING TECHNIQUES</p> <p>Remotely triggered black hole (RTBH) filtering can drop undesirable traffic before it enters a protected network. Network black holes are places where traffic is forwarded and dropped. When an attack has been detected, black holing can be used to drop all attack traffic at the network edge based on either destination or source IP address</p> <p>Unicast Reverse Path Forwarding</p> <p>Network administrators can use Unicast Reverse Path Forwarding (uRPF) to help limit malicious traffic flows occurring on a network, as is often the case with DDoS attacks. This security feature works by enabling a router to verify the "reachability" of the source address in packets being forwarded. This capability can limit the</p> |

appearance of spoofed addresses on a network. If the source IP address is not valid, the packet is discarded.

To enable uRPF, enter this command:

```
hostname(config)#ip verify reverse-path interface  
interface_name
```

GEOGRAPHIC DISPERSION

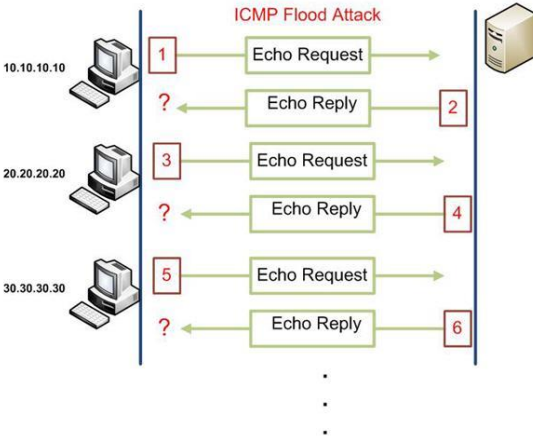
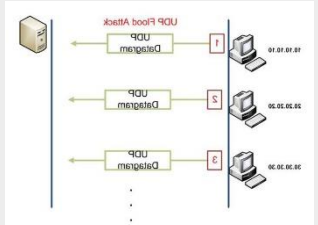
Anycast is a routing methodology that allows traffic from a source to be routed to various nodes (representing the same destination address) via the nearest hop/node in a group of potential transit points. This solution effectively provides "geographic dispersion."

Tightening Connection Limits and Timeouts

Antispoofing measures such as limiting connections and enforcing timeouts in a network environment seek to ensure that DDoS attacks are not launched or spread from inside the network either intentionally or unintentionally. Administrators are advised to leverage these solutions to enable Antispoofing and thwart random DDoS attacks on the inside "zones" or internal network. Oversubscription of stateful processes can cause a device to fail.

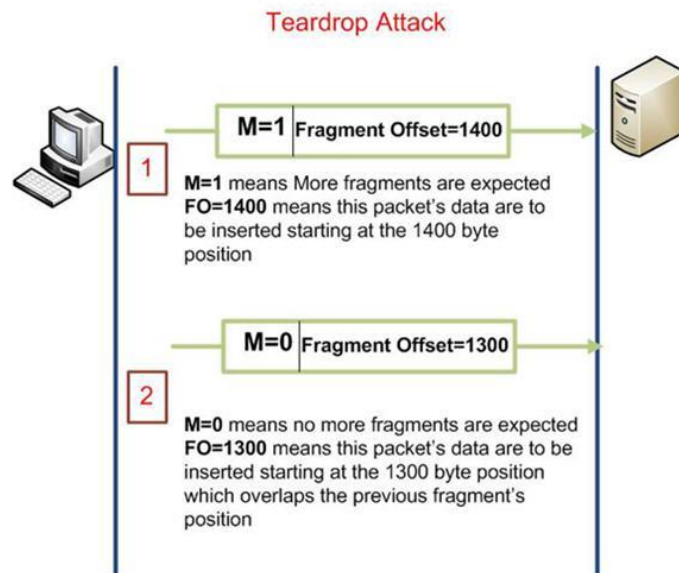
Access Control Lists

ACLs provide a flexible option to a variety of security threats and exploits, including DDoS. ACLs provide day zero or reactive mitigation for DDoS attacks, as well as a first-level mitigation for application-level attacks. An ACL is an ordered set of rules that filter traffic. Each rule specifies a set of conditions that a packet must satisfy to match the rule. Firewalls, routers, and even switches support ACLs. When the device determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether the packet is permitted or denied. If there is no match, the switch applies the applicable default rule (generally an implicit "deny all"). The device continues processing packets that are permitted and drops packets that are denied.

| | | |
|----|---|---|
| | | |
| 66 | ICMP Flood Attack | <p>Similar to the SYN Flood attack, an ICMP flood takes place when an attacker overloads its victim with a huge number of ICMP echo requests with spoofed source IP addresses.</p> <p>The simplest one was to completely disable ICMP from untrusted interfaces and the more complicated one was to policy the rate of transmission of ICMP requests and limit down this rate in case of aggression.</p> <p>This is how the attack is performed.</p>  |
| 67 | UDP Flood Attack | <p>UDP flooding doesn't differ from ICMP flooding. The idea behind these attacks is the same and we have already talked about it. The only difference in this case is the fact that the IP packets that the attacker uses against its victim contain UDP datagrams of different sizes.</p>  |
| 68 | Tear drop attack (IP Fragmentation Attack) | <p>This type of attack deals with fragmentation and reassembly of IP packets. The IP header contains the necessary fields to handle fragmentation issues. Basically there are three fields within an IP datagram related to fragmentation and reassembly; these area:</p> <ul style="list-style-type: none"> • Do not fragment bit • More fragments bit • Fragment Offset <p>The Fragment Offset field, which is the crucial field in our case, is used to indicate the starting position of each fragment relative to the</p> |

original unfragmented packet. An attacker could start transmitting fragmented IP packets containing overlapped Fragment Offsets making the victim unable to reassemble them exhausting the victim's resources and possibly crashing it.

The following diagram will help you understand how this attack is utilized:




Mitigations:

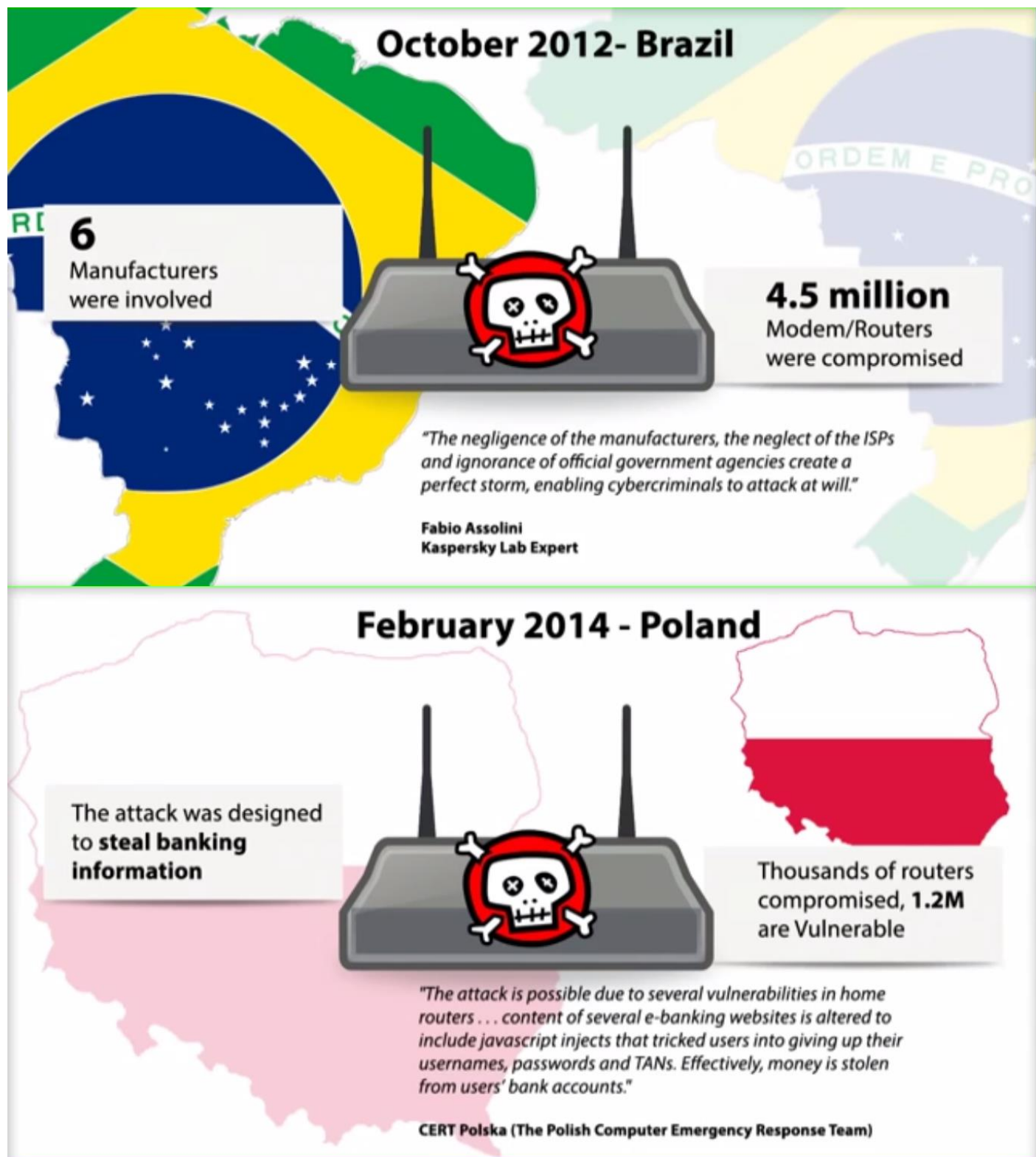
Inspecting incoming packets for fragmentation rules, these inspections are augmented by DDoS protection hardware.

| | | |
|----|--|--|
| 69 | MITM (Man in The Middle Attack) | <p>Here the attacker manages to intercept the data flowing from a source to a destination. The attacker can simply read the data or even modify the data. Such an attack can be carried out in many ways. One of them is using - ICMP redirect for a router. ICMP redirect packets are actually sent by routers to hosts if they find a better path to reach a destination. If a router receives a packet and forwards the packet to the same interface where it had received, then an ICMP redirect can be sent. But an attacker can carry a man in middle attack using redirects.</p> <p>MITIGATIONS:</p> <p>1>Firewall (packet filter): it prevents the malicious packets from entering into the network. firewalls are typically located outside the network security parameter as the first line of defence.</p> |
|----|--|--|

| | | |
|----|---|---|
| | | <p>2>Network Address Translation(NAT): hides the ip of network device from the attacker the computer in a network where NAT assigns ip address are assigned special IP Address.</p> <p>3>Demilitarized Zone(DMZ): Another network that sits outside the protected network parameter. Outside users can access the DMZ but cannot enter the secure network.</p> |
| 70 | Unknown Logins | Attackers who do not have direct physical access to a router can crack the routers telnet password and log into the router and reconfigure it which can make the router act maliciously. |
| 71 | TCP Reset Attack | <p>Tcp reset attack is the attack in which a tcp connection is terminated by the attacker using a spoofed packet with the RST (reset) bit in the tcp packet set. To carry out this attack, the attacker simply sniffs the tcp connection to get the source ip address, source port number, destination ip address, destination port number and most importantly the ongoing sequence number. Now the attacker creates a fake tcp packet with proper source ip and port and destination ip and port. The sequence number is also filled appropriately. The RST bit in this packet is set. When this packet reaches destination, it sees that the RST bit is set and hence it terminates the connection. So the continuity is disrupted until an entire new tcp session is established. This is certainly not desirable. The severity of this attack varies from application to application. For example, Cisco's BGP protocol is highly affected by this attack. BGP is the protocol that runs in the service provider architecture and has to manage huge routing tables. Whenever a route goes down, BGP does a lot of processing over many routers to fix the problem. In this case if the tcp attack is carried out, bgp will do a lot of processing because of the terminated connection. If a connection is terminated frequently, bgp also gradually isolates that router from the network because it is held responsible for causing a lot of processing frequently over many routers. So a harmless router can be isolated because of such an attack.</p> |
| 72 | Attacks on OSPF(open short path first) | <p>1. Hello packets dropped: OSPF neighbours are formed by exchanging hello packets. These hello are not acknowledged by the other end. When OSPF misses certain hello packets, the neighbour is considered as dead. This depends on dead timer of</p> |

| | | |
|----|-------------------|---|
| | | <p>OSPF. An attacker can purposely delete some OSPF packets. This will cause the neighbour to be declared as dead.</p> <p>2. Max Sequence attack: OSPF sends LSAs (Link State Update) to exchange routing information with their neighbours. LSA contains a sequence number which helps the router determine as to which one is the freshest route. An attacker can send LSA containing the max sequence number which is 0x7FFFFFFF. Thus all routers will accept this as the freshest update. This update will stay in the LSDB (Link State Database) for one hour thus helping the attacker to harm the network within that period.</p> <p>3. Attacking external routes: Routes that come from external areas or autonomous systems are trusted. Such routes are not checked for validity. So an attacker can send false external routes which will not be validated.</p> |
| 73 | Link Bleed | <p>This was first observed in the LINKGEAR WRG716. It allows hackers to modify the DNS Settings.</p>  |

Sometimes It's due to negligence of Manufacturers and ISP...



January 2014 - Vietnam

D-Link, Micronet,
Tenda, TP-Link routers
were involved



300,000
Routers were
compromised

"As the bar is increasingly raised for compromising endpoint workstations, cyber criminals are turning to new methods to achieve their desired goals"

Team Cymru

CONCLUSION

Different types of attacks are targeted towards the router. Various security mechanisms are devised to protect the router from such attacks. Log analysis can also be one such method for router security. But the logs that are sent over the network use the UDP (user datagram protocol). UDP is not reliable. Hence some log packets can be lost. Some mechanisms can be done to prevent loss from such failure. Also the log formats might change for different IOS (Cisco's Internetwork Operation System). So a way can be found to deal with these changes also. Thus automated log analysis can help us remove all the noise from the logs and actually concentrate on only the important entries for network management and security.

REFERENCES

Charalampos Patrikakis, Michalis Masikos, and Olga Zourarak, DISTRIBUTED DENIAL OF SERVICE ATTACKS, The Internet Protocol Journal - Volume 7, Number 4, 2004.

ICMP Attacks Illustrated, SANS Institute InfoSec Reading Room

Michael Sudkovitch and David I. Roitman, OSPF Security project book, 2010.

Danai Chasaki and Tilman Wolf, ATTACKS AND DEFENSES IN THE DATA PLANE OF NETWORKS, IEEE transactions on dependable and secure computing (tdsc), 2012.

Kirk A.Radley, Steven Cheung, Nicholas Puketza, Biswanath Mukherjee, and Ronald A. Olsson, DETECTING DISRUPTIVE ROUTERS: A DISTRIBUTED NETWORK MONITORING APPROACH.

Vrizlynn L. L. Thing, Morris Sloman, Naranker Dulay, LOCATING NETWORK DOMAIN ENTRY AND EXIT POINT/PATH FOR DDOS ATTACK TRAFFIC.

Muhammad Naveed, Shams un Nihar, Mohammad Inayatullah Babar, NETWORK INTRUSION PREVENTION BY CONFIGURING ACLS ON THE ROUTERS, BASED ON SNORT IDS ALERTS, Emerging Technologies (ICET), 2010.

Anand Deveriya, An overview of the Syslog protocol, Cisco Press, 2005.

Karsten Iwen, Logging in Cisco IOS.

Sean Wilkins, Basic access lists configuration for cisco devices, Cisco Press, 2011.

Cisco IOS Debug Command Reference, Release 12.3.

<http://www.tripwire.com/state-of-security/vulnerability-management/ruckus-vulnerability/>

