TCP/IP Exploits

Format

Exploit Name

Student Name(s):
URL:
Description:

Source Address Spoofing

Student Name(s): Justin Pilecki
URL: https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture16.pdf
Description: Malicious user has a forged source IP address that can launch a flood attack on some host from another network. In this scenario forwarded packets have their IP address field overwritten, hiding the true IP of the user. This could be used as the basis for DoS or SYN/ACK floods.

Sockstress

Student Name(s): Jordan Abbott
URL:https://en.wikipedia.org/wiki/Sockstress
Description: A type of denial-of-service attack which exploits zero/small window sizes and other methods to cause stress on the web server using minimal traffic. For example, one type of attack can be done by sending an ACK packet with a window size of 0, which causes the server to "probe" the client, looking for data on that window. The result is that the connection remains open indefinitely.

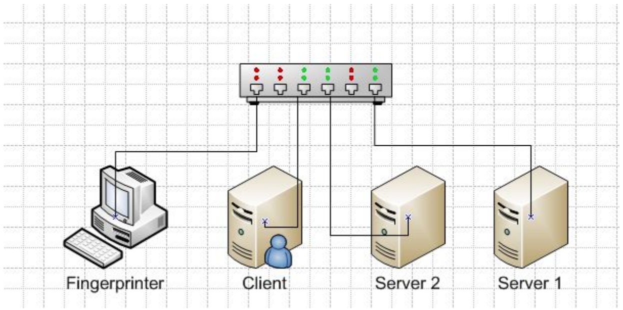
TCP Reset Attack

Student Name(s): Robert Airth
URL: https://robertheaton.com/2020/04/27/how-does-a-tcp-reset-attack-work/
Description: This type of attack uses spoofing to send RST (reset) messages to one or both hosts engaged in a TCP connection. This attack is said to be used in China's "The Great Firewall" to be able to kill a TCP connection after monitoring/collecting data about the client hosts habits. This attack generally requires a long-lived TCP connection, as the ability to reset a short-lived connection has low probability due to the inherent speed of the connection. The blind spoofing process requires spoofing the correct sequence numbers for the RST to be accepted.

Exploit Name DNS amplification attack
Student Name(s): Edmar Ramos
URL: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/
Description: its similar to DDOS attack. A bot on a client request packet from a spoof ip address. This attacks both client and server

TCP Stack Fingerprinting

Student Name(s): James Pelligra
URL: https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting
Description: The passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote machine's operating system (aka, OS fingerprinting), or incorporated into a device fingerprint. Used for reconnaissance by malicious users. Happens when the fingerprinting device has access to the same network that the client and server are on.



Exploit Name

Student Name(s): Fernando Crespo
URL:
https://blogs.blackberry.com/en/2018/08/modern-cell-networks-are-vulnerable-to-nasty-lte-exploit , https://www.acunetix.com/blog/web-security-zone/what-is-cookie-poisoning/
Description: the first link talks about the exploitation of LTE cell phone towers by using ismi catchers to create a “fake” cell phone tower to catch information from cell phone users within a 2km radius. The second link talks about cookie poisoning and how a malicious user exploits cookies in a website so when a user accesses that website their information can be hijacked.

Exploit Name

Student Name(s): Stephen Zazueta
URL:https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/#:~:text=What%20is%20a%20SYN%20flood,consuming%20all%20available%20server%20resources

Description: SYN Flood attack. Type of DDOS attack (server resources are all consumed) where SYN packets are sent from spoofed IP addresses in high volumes. The victim server keeps responding and opening ports but doesn't receive ACK. Once all ports are utilized, the server is unavailable.

List of Possible Exploits

Student Name(s): Jay Revolinsky
URL: https://www.informit.com/articles/article.aspx?p=361984&seqNum=10
Description: An article that shows a list of the possible internet exploits used in 2005 to run malicious programs on a victim's computer. More abstract than technical but makes for a relatively comprehensive list. My favorite, "**Byzantine attack**: Here, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, routing packets on non-optimal paths, and selectively dropping packets [17]. Byzantine failures are hard to detect. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be exhibiting Byzantine behavior."

Command Injection attack

Student Name(s):Silvestre
URL: https://hacksland.net/reverse-tcp-shell-with-metasploit/
https://www.hackingarticles.in/command-injection-exploitation-using-web-delivery-linux-windows/
Description: Explains the difference between a reverse TCP shell and a bind TCP shell. A reverse TCP shell can be used to bypass firewall restrictions on open ports and can be used for a command injection attack.

Tcp Blind Spoofing

Student Name(s): Jacob Castro
URL:
https://www.blackhat.com/docs/us-16/materials/us-16-Nakibly-TCP-Injection-Attacks-in-the-Wild-A-Large-Scale-Study.pdf
Description: Here, an attacker is able to guess both the sequence number of an ongoing communication session and its port number. They are then in a position to carry out an injection attack

Exploit Name: DNS Spoofing

Student Name(s): Summer Banister
URL: https://www.imperva.com/learn/application-security/dns-spoofing/
Description: With DNS spoofing, a malicious entity will modify a DNS server so that a specific domain name is rerouted to a different IP address. This new IP address will be for a server controlled by the attacker, and can be used to steal personal information (like access credentials) and spread computer worms and viruses.

Exploit Name

Student Name(s): Justin
URL:

Description: Reflection SYN attack

Student Name(s): Jack Lambert

URL:https://www.ionos.com/digitalguide/server/security/syn-flood/ - description: A detailed description of SYN attacks, a class of DoS attacks, and their possible mitigations is discussed. A SYN attack involves sending large numbers of illegitimate SYSYN packets without acknowledging them, resulting in the server keeping resources allocated for 'half open' connections. The articles also shows a specific variant called a reflection SYN flood attack,which takes advantage of the fact that servers often respond to one SYN with multiple SYN/ACK packets to multiply the network traffic caused by a SYN attack, achieving the goals of a DoS attack by consuming network resources instead of server resources.

TCP Sequence Number Prediction

Student Name: Brian Buchmiller
URL: https://www.cs.columbia.edu/~smb/papers/ipext.pdf
Description: By initiating a handshake with the server from a client, the user can find the ISN (initial sequence number). Due to how ISN's are generated it is possible to calculate what the next ISN will be and inject data or terminate/hijack sessions from other clients. This can be countered by making the ISN more unpredictable - through more randomization or quicker cycles.

Exploit Name

Student Name(s): Candace Moore
URL: https://www.cs.columbia.edu/~smb/papers/ipext.pdf
Description: This research paper describes in the first few pages the vulnerabilities that are associated with the 3 way handshake. Some of these flaws exist because hosts rely on IP source addresses for authentication. Others exist because network control mechanisms, particularly routing protocols, have minimal or non-existent authentication.

Exploit Name

Student Name(s): Bradley Arline
URL: https://www.cvedetails.com/cve/CVE-2015-2370/
Description: An Microsoft RPC subsystem Exploit that allowed a user to gain local access remotely on a microsoft machine.

Smurf Attack

Student Name(s): Riley Heffernan
URL: https://www.kaspersky.com/resource-center/definitions/what-is-a-smurf-attack
Description: A smurf attack exploits PING packets using the ICMP protocol to create an infinite loop of data flowing on a network. This is enough to DoS not just a single machine, but entire organizations. Often, the attack is executed using a trojan or similar program on an infected machine to create a persistent issue. The primary solution to this problem is reconfiguration of the router to disallow IP broadcasting

Exploit Name

Student Name(s): Justin
URL:
Description:

Exploit Name

Student Name(s): James Schulz
URL: https://us-cert.cisa.gov/ncas/archives/alerts/TA04-111A
Description: If you can predict the approximate sequence number range of packets, you can inject packets into the stream.

Treck TCP/IP Stack Vulnerabilities

Student Name(s): Grayson Beckert
URL:
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-treck-tcpip-stack-could-allow-for-remote-code-execution_2020-083/
Description: Multiple vulnerabilities in theTreck TCP/IP Stack called Ripple20, the worst of which results in remote code execution and remote control of a device within a network.

TCP RST Attacks on Video Streaming Applications:

Student Name(s): Kevin Tieu
URL:https://www.utc.edu/center-academic-excellence-cyber-defense/pdfs/course-paper-5620-attacktcpip.pdf
Description: Similar to TCP RST attacks on Telnet and SSH. One addition was that the GUI of the browser showed that the connection to the video source continued to try to reconnect after the TCP RST message

TCP Spoofing Attack/Spoof Session Flood/Fake Session Attack:

Student Name(s): Kevin Tieu
URL:https://www.securitymagazine.com/articles/92327-are-you-ready-for-these-26-different-types-of-ddos-attacks
Description: In order to circumvent network protection tools, the attacker may forge a TCP session by submitting a bogus SYN packet, a series of ACK packets, and at least one RST (reset) or FIN .

TCP RST Attacks on telnet and ssh Connections:

Student Name(s): Kevin Tieu
URL:https://www.utc.edu/center-academic-excellence-cyber-defense/pdfs/course-paper-5620-attacktcpip.pdf
Description: an attacker continually sends TCP RST packets to a target IP and port number which will effectively prevent any communication on that port.

Transport Layer Attacks
Student Name(s): Kierstyn Hughes
URL: https://flylib.com/books/en/2.902.1.13/1/
Description: Gives examples of TCP being exploited at the Transport Layer, Network Interface Layer, Internet Layer, and Application Layer (May be old, since last update, I believe, is from 2017).

- “Attacks at the Transport layer can take advantage of the TCP and UDP protocols and the various implementations of those protocols. Examples of this type of attack would be sending the ending sequence of a TCP three-way handshake, or sending a packet that is larger than the largest supported packet size.” Examples of attacks include:
- Manipulation of the UDP or TCP ports.
- Denial of Service (DoS).
- Session hijacking.

Connection Hijacking

Student Name(s): Peter Boster
URL: http://cecs.wright.edu/people/faculty/pmateti/InternetSecurity/Lectures/TCPexploits/
Description: “YY trusts the packets from XX because of its correct SEQ/ACK numbers. So if there was a way to mess up XX's SEQ/ACK, YY would ignore XX's real packets. Attacker could then impersonate to be XX, but using correct SEQ/ACK numbers from the perspective of YY. The attacker can confuse XX's SEQ/ACK numbers as seen by YY by simply inserting a data packet into the stream at the right moment (ZZ as XX->YY). YY would accept this data, and update ACK numbers. XX would continue to send it's old SEQ numbers, as it's unaware of our spoofed data. This results in ZZ hijacking the connection: host XX is confused, YY thinks nothing is wrong as ZZ sends 'correct' packets to YY. Each time a packet arrives at YY out of sequence from the real XX, the YY answers it with 'correct' SEQ/ACK.”

Off-Path TCP Wi-Fi Exploit

Student Name(s): Vanja Venezia
URL: https://www.cs.ucr.edu/~zhiyunq/pub/sec18_TCP_offpath_wifi.pdf
Description: General set of exploits utilizing the Global IPID counter that Windows used to use for TCP but modified to work with 802.11. A side channel is essentially created by the global counter in Windows, attackers could check whether or not their spoofed IP is correct by observing the server response via this side channel. This same confirmation can be achieved via the timing channel in 802.11, as it can be referenced to see the RTT effect from a sent packet. This allows attackers to see the delay effect their spoofed packet causes, thus confirming whether or not an IP has been chosen correctly and leveraging the TCP packet

validation logic. This setup allows for web cache poisoning, however many attacks can be launched from this point.