CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

Common Network Attacks

Chris Samayoa

Week 12 – 2nd Lecture
4/7/2022

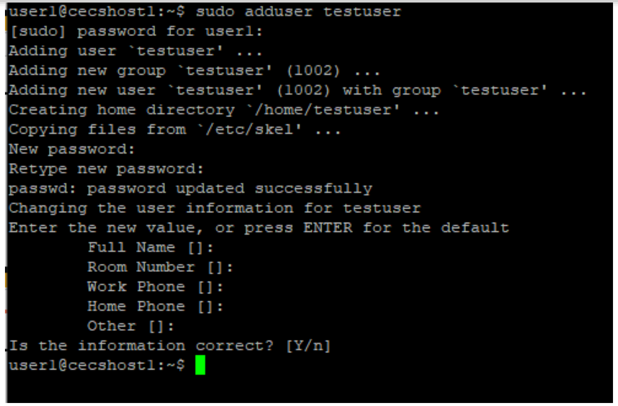
Course Information

- CECS 303
  - Networks and Network Security – 3.0 units
- Class meeting schedule
  - TuTH 5:00PM to 7:15PM
  - Lecture Room: VEC 402
  - Lab Room: ECS 413
- Class communication
  - chris.samayoa@csulb.edu
  - Cell: 562-706-2196
- Office hours
  - Thursdays 4pm-5pm (VEC-404)
  - Other times by appointment only

Objectives

- Linux commands
- Common Network Attacks – Overview
- Malware
- DDOS
- SQL Injection Attacks

Linux Commands

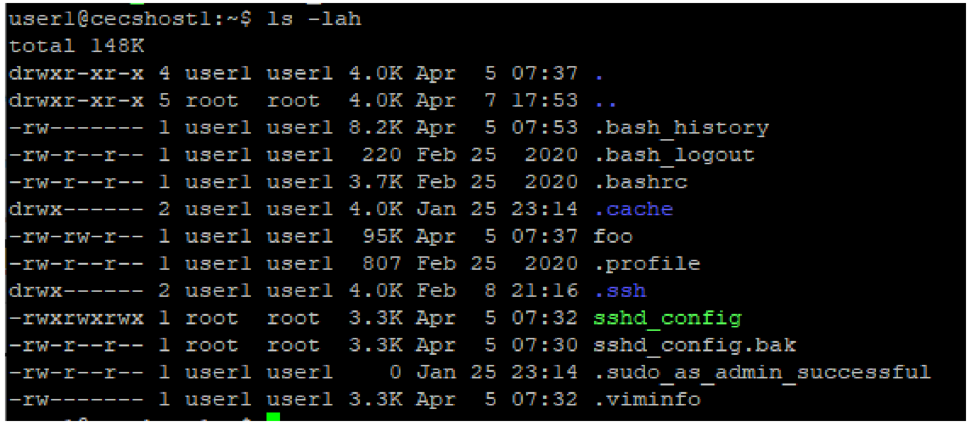


```
user1@cecshost1:~$ sudo adduser testuser
[sudo] password for user1:
Adding user `testuser' ...
Adding new group `testuser' (1002) ...
Adding new user `testuser' (1002) with group `testuser' ...
Creating home directory `/home/testuser' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for testuser
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
user1@cecshost1:~$
```

- Add a user
  - ‘sudo adduser [username]’
  - Reset password: ‘sudo passwd [username]’
- Copy a file
  - ‘sudo cp’
  - e.g. ‘sudo cp /var/log/syslog /var/log/syslog.bak’
    - If no file path is specified, the command uses the path you are currently in
- Modify file permissions
  - ‘sudo chmod [permissions] [file name]’
- Additional commands from lab 6
  - sudo /usr/sbin/sshd -f sshd_config -p 2222 &
    - Starts additional ssh process using modified ssh_config and TCP port 2222
    - ‘&’ tells the process to run in the background
  - sudo ss –ntlp
    - ‘ss’ command is used to show socket information
    - This is used in the lab to verify the previous command was successful

Linux Command: chmod

- Three groups of permissions
  - owner
  - group
  - others (public)
- Symbolic notation
  - e.g. “-rwxr-xr--”
    - ➢ First character represents file type (file or directory)
    - ➢ Next 9 characters represent read (r), write (w), and execute (x) permissions for owner, group, and others respectively
- Numeric notation
  - Each digit represents owner, group, and others respectively
  - e.g. ‘sudo chmod 777 [file name]’
    - 0: No permission
    - 1: Execute
    - 2: Write
    - 3: Write and execute
    - 4: Read
    - 5: Read and execute
    - 6: Read and write
    - 7: Read, write, and execute



```
user1@cecshost1:~$ ls -lah
total 148K
drwxr-xr-x 4 user1 user1 4.0K Apr  5 07:37 .
drwxr-xr-x 5 root  root  4.0K Apr  7 17:53 ..
-rw------- 1 user1 user1 8.2K Apr  5 07:53 .bash_history
-rw-r--r-- 1 user1 user1  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 user1 user1 3.7K Feb 25  2020 .bashrc
drwx------ 2 user1 user1 4.0K Jan 25 23:14 .cache
-rw-rw-r-- 1 user1 user1  95K Apr  5 07:37 foo
-rw-r--r-- 1 user1 user1  807 Feb 25  2020 .profile
drwx------ 2 user1 user1 4.0K Feb  8 21:16 .ssh
-rwxrwxrwx 1 root  root  3.3K Apr  5 07:32 sshd_config
-rw-r--r-- 1 root  root  3.3K Apr  5 07:30 sshd_config.bak
-rw-r--r-- 1 user1 user1    0 Jan 25 23:14 .sudo_as_admin_successful
-rw------- 1 user1 user1 3.3K Apr  5 07:32 .viminfo
```

Linux Tool: strace

- Purpose: process monitoring, diagnostic, and debugging tool for Linux
- Uses:
  - Debugging Programs
  - Troubleshooting Programs
  - Intercept System calls by a process
  - Record system calls by a process
  - Record signals received by a process
  - Trace running processes
- Examples:
  - https://www.geeksforgeeks.org/strace-command-in-linux-with-examples/
  - 'sudo strace –p [process ID]'
    - Process ID can be determined by examining the results of a 'sudo ps' command in Linux (or 'sudo ps aux' to use the format used in Lab 6)
      - 'a' flag = show processes for all users
      - 'u' flag = show process's user/owner
      - 'x' flag = show processes not attached to a terminal

Dirty Pipe

- Linux privilege escalation vulnerability
  - URL with more information: https://arstechnica.com/information-technology/2022/03/linux-has-been-bitten-by-its-most-high-severity-vulnerability-in-years/
  - CVE-2022-0847 (https://nvd.nist.gov/vuln/detail/CVE-2022-0847)
  - CVSS: 7.8
  - This is a local privilege escalation bug
- Background information
  - A Linux 'pipeline' is a mechanism for one process to send data to another process
  - Name was derived from a previous Linux local privilege escalation bug that became well known Dirty Cow (https://arstechnica.com/information-technology/2016/10/most-serious-linux-privilege-escalation-bug-ever-is-under-active-exploit/)
  - Essentially, the exploit allows any user (including underprivileged ones) to overwrite data to any file that the user has 'read' access to using a 'pipe' they create
- What can they do?
  - Create a new user with root privileges
  - First proof-of-concept added additional SSH key to root user's account
    - This allows a remote connection to be established with root privileges
  - The integrity of any readable file on the system could be compromised
  - Lab 6 – strace exercise?

Objectives

- Linux commands
- Common Network Attacks – Overview
- Malware
- DDOS
- SQL Injection Attacks

Common Network Attacks

- Malware
  - Malicious software that is used to exploit devices at the expense of victim resources
- Distributed Denial of Service Attack (DDOS)
  - An attack where multiple (typically compromised) systems attack a target with the goal being to overwhelm the resource and make it unavailable for use
- SQL Injection Attacks
  - Attackers can construct a web request that provides unintended access to database resources
  - Can be used to create, modify, delete, or extract data from a database
- Cross-site Scripting (XSS) Attack
  - Attacker injects a malicious script into a trusted website
  - Injected script will then be delivered to a victim’s web browser
  - Used to spread malware, steal credentials, or steal user sessions
- Man-in-the-Middle Attack
  - Attacker intercepts communications between two or more parties to intercept data
- DNS Tunneling
  - Command-and-control tactic that uses DNS queries to go undetected
- Email Attacks

Objectives

- Linux commands
- Common Network Attacks – Overview
- Malware
- DDOS
- SQL Injection Attacks

Malware

- Intent
  - While malware can perform any action it is programmed to do, the goal is typically to perform these actions while maintaining persistent network access for the attacker
- According to Statista – Malware attacks peaked in 2018 at 10.5 billion and had dropped to 5.6 billion by 2020
  - Ransomware attacks have grown exponentially during this time

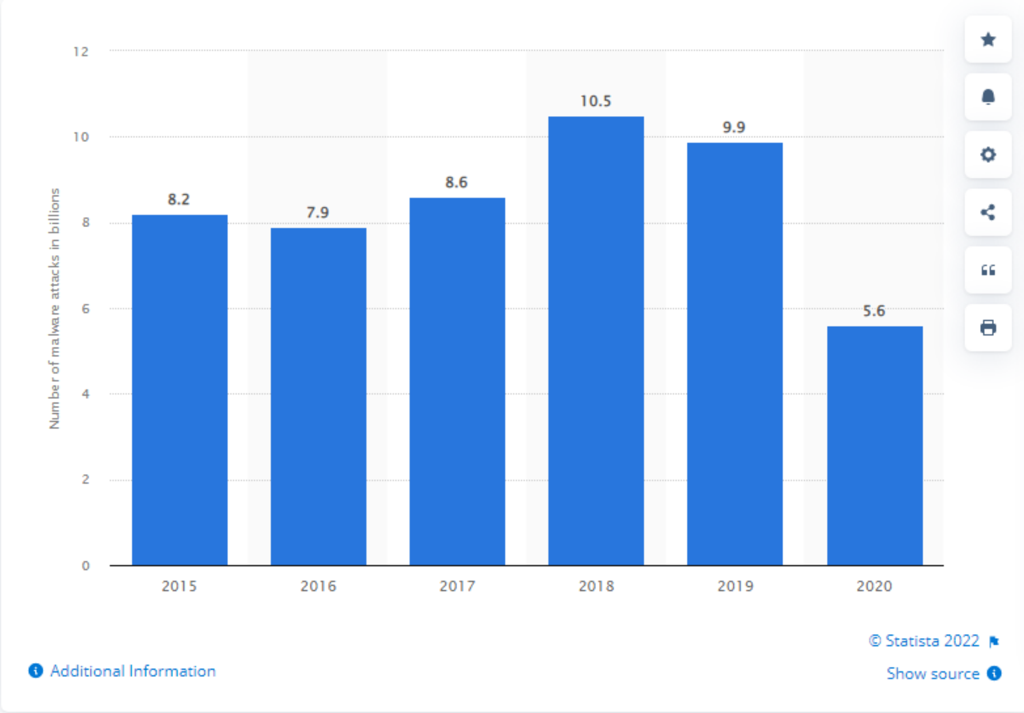


Image: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/#professional

Malware Types

- Virus / Worm
- Trojan Horse
  - Program that is downloaded and installed on a device that is believed to be trusted, but is actually malicious
  - e.g. Free program downloads or email attachments
- Spyware
  - Any malicious software that monitors a user's activity on a given device without their knowledge
  - e.g. Internet activity, credentials, and other sensitive information
  - Can perform reconnaissance for government agencies or criminal organizations
- Ransomware
  - Malicious software designed to encrypt a target's files and then demand a ransom to receive a decryption key
  - Often used in conjunction with extortion – Pay us or we leak your data online

Malware Examples

- SolarWinds
  - https://www.networkworld.com/article/3600833/trojan-in-solarwinds-security-has-far-reaching-impact.html
  - Attributed by FireEye to a nation-state action
    - Russian according to Reuters
  - Supply chain attack
  - Trojan would remain dormant for 12-14 days prior to reaching out to a command-and-control server
  - Solarwinds had over 300,000 customers at the time
    - 425 of the U.S. Fortune 500
    - Pentagon, NSA, DoJ, and others included
- WannaCry
  - https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware
  - Used EternalBlue vulnerability to spread as a worm
    - https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/
    - CVE-2017-0144
    - CVSS Score: 8.1
    - Affected Windows operating systems with outdated SMB versions (TCP port 445)
  - Most that paid never received decryption keys
  - Symantec estimated that the losses from this attack amounted to $4 - $5 billion
  - “Kill Switch” found by MalwareTech provided temporary relief (https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/)

Objectives

- Linux commands
- Common Network Attacks – Overview
- Malware
- DDOS
- SQL Injection Attacks

DDOS

- Purpose
  - Compromise the availability of a target (e.g. server or website)
  - Can take the form of flooding with traffic or any other exploited vulnerability that crashes the system
- Prevalence
  - Attacks increased by 15% in first half of 2020 to 4.83 million (Help Net Security)
    - ➢ Largest attack in 1 hour was 1.12 TBPS (per their available data)
    - ➢ 92% of attacks were for less than an hour – 51% decrease in duration from 2019
- Costs
  - Vary by size of business
  - Ransom / extortion

DDOS (cont'd)

- Denial of Service (DoS)
  - Attack comes from a single source
  - DDOS is distributed, meaning that the attack comes from multiple systems working together towards a specific target
    - More volume available to contribute to the attack
    - Harder to track since there are more systems involved
    - Harder to stop / shut down
    - Harder to find originator of attack
- How
  - Buffer overflow attack – more traffic is sent that can be handled by the system
  - Smurf Attack
  - Ping of Death
  - SYN Flood
    - Overwhelms target with SYN packets, handshake is not completed, but all open ports are saturated with SYN requests

DDOS (cont’d)

- Smurf Attack
  - Defined:
    - Attacker crafts a packet that spoofs the real IP address of the intended target
    - Packet is sent to broadcast address of subnet – which is then distributed by a router or firewall to all devices on that network subnet
    - Each device on subnet receives the request and responds to spoofed address with ICMP echo reply packet
    - Target receives all of these ICMP echo reply packets and can be overwhelmed
  - Has mainly been mitigated in modern networks
    - Ability to initiate messages to the broadcast address is typically disabled by default now on routers
- Ping of Death
  - Was performed by sending a malformed packet to a network device that when assembled was larger than the allowed size of 65,535 bytes using ping commands (violates internet protocol)
    - This used to be enough to crash network hardware previously (buffer overflow)
    - Was also used to overwhelm targets that became overwhelmed trying to put fragmented malformed packets together
  - Mitigated in late 90s by better designed network devices and operating systems

DDOS Example

- Microsoft mitigates 2.4Tbps DDoS Attack
  - https://www.theverge.com/2021/10/12/22722155/microsoft-azure-biggest-ddos-attack-ever-2-4-tbps
  - Involved 70,000 sources within Asia-Pacific region and United States
  - Shows another benefit to using cloud solutions
- Many other examples available online that have tested edge and cloud providers
- Success of these attacks are likely higher on small businesses that run their infrastructure on premises

Objectives

- Linux commands
- Common Network Attacks – Overview
- Malware
- DDOS
- SQL Injection Attacks

SQL Injection

- Purpose
  - Craft calls to web server with the intention of having malicious instructions sent to a SQL server in the backend
- Potential Impacts
  - Database corruption
  - Authentication bypass
  - Data tampering / modification (integrity issue)
  - Data theft / exfiltration (confidentiality issue)
  - Deletion of data
  - Arbitrary code execution
  - Complete compromise of system (root access)

SQL Injection (cont’d)

- Continued next lecture