Pramodh Krishna

Aug 22, 2023 20% knowledge

Data Sanity

Aug 23, 2023

Top 10 Most Notorious Hackers of All Time

1. Kevin Mitnick

Hacked the North American Defense Command (NORAD), Digital Equipment Corporation's (DEC) network, Pacific Bell
Grey hat hacker

2. Anonymous

Black Hat hackers group

3. Adrian Lamo

He hacked The New York Times' intranet, added himself to the list of expert sources and began conducting research on high-profile public figures. Grey Hat Hacker

4. Albert Gonzalez

Gonzalez was arrested in New York for debit card fraud related to stealing data from millions of card accounts.
During his time as a paid informant, Gonzalez continued his in criminal activities. Along with a group of accomplices, Gonzalez stole more than 180 million payment card accounts from companies including OfficeMax, Dave and Buster's and Boston Market.
Complete Black Hat HAcker

5. Matthew Bevan and Richard Pryce

Matthew Bevan and Richard Pryce are a team of British hackers who hacked into multiple military networks in 1996, including Griffiss Air Force Base, the Defense Information System Agency and the Korean Atomic Research Institute (KARI). Bevan (Kuji) and Pryce (Datastream Cowboy) have been accused of nearly starting a third world war after they dumped KARI research onto American military systems. Bevan claims he was looking to prove a UFO conspiracy theory, and according to the BBC, his case bears resemblance to that of Gary McKinnon. Malicious intent or not, Bevan and Pryce demonstrated that even military networks are vulnerable.

Grey Hat HAcker

6. Jeanson James Ancheta

Jeanson James Ancheta had no interest in hacking systems for credit card data or crashing networks to deliver social justice. Instead, Ancheta was curious about the use of bots—software-based robots that can infect and ultimately control computer systems. Using a series of large-scale "botnets," he was able to compromise more than 400,000 computers in 2005. According to Ars Technica, he then rented these machines out to advertising companies and was also paid to directly install bots or adware on specific systems. Ancheta was sentenced to 57 months in prison. This was the first time a hacker was sent to jail for the use of botnet technology.

Black Hat Hacker

7. Michael Calce

In February 2000, 15-year-old Michael Calce, also known as "Mafiaboy," discovered how to take over networks of university computers. He used their combined resources to disrupt the number-one search engine at the time: Yahoo. Within one week, he'd also brought down Dell, eBay, CNN and Amazon using a distributed-denial-of-service (DDoS) attack that overwhelmed corporate servers and caused their websites to crash. Calce's wake-up call was perhaps the most jarring for cyber crime investors and internet proponents. If the biggest websites in the world—valued at over $1 billion—could be so easily sidelined, was any online data truly safe? It's not an exaggeration to say that the development of cyber crime legislation suddenly became a top government priority thanks to Calce's hack.

Black Hat Hacker

8. Kevin Poulsen

In 1983, a 17-year-old Poulsen, using the alias Dark Dante, hacked into ARPANET, the Pentagon’s computer network. Although he was quickly caught, the government decided not to prosecute Poulsen, who was a minor at the time. Instead, he was let off with a warning.

Poulsen didn’t heed this warning and continued hacking. In 1988, Poulsen hacked a federal computer and dug into files pertaining to the deposed president of the Philippines, Ferdinand Marcos. When discovered by authorities, Poulsen went underground. While he was on the run, Poulsen kept busy, hacking government files and revealing secrets. According to his own website, in 1990, he hacked a radio station contest and ensured that he was the 102nd caller, winning a brand new Porsche, a vacation, and $20,000.

Poulsen was soon arrested and barred from using a computer for three years. He has since converted to white hat hacking and journalism, writing about cyber security and web-related socio-political causes for Wired, The Daily Beast and his own blog Threat Level. Paulson also teamed with other leading hackers to work on various projects dedicated to social justice and freedom of information. Perhaps most notably, working with Adam Swartz and Jim Dolan to develop the open-source software SecureDrop, initially known as DeadDrop. Eventually, Poulsen turned over the platform, which enabled secure communication between journalists and sources, to the Freedom of Press Foundation.

Black Hat Hacker

9. Jonathan James

According to the New York Times, what really earned James attention was his hack into the computers of the United States Department of Defense at 15 His hacking allowed him to access over 3,000 messages from government employees, usernames, passwords and other sensitive data.
James became the youngest person to be convicted of violating cybercrime laws. In 2007, TJX, a department store, was hacked and many customer’s private information were compromised by James

Black Hat Hacker

10. ASTRA

This hacker differs from the others on this list in that he has never been publicly identified. However, according to the Daily Mail, some information has been released about ASTRA. Namely that he was apprehended by authorities in 2008, and at that time he was identified as a 58-year-old Greek mathematician. Reportedly, he had been hacking into the Dassault Group, for almost half a decade. During that time, he stole cutting edge weapons technology software and data which he then sold to 250 individuals around the world. His hacking cost the Dassault Group $360 million in damages. No one knows why his complete identity has never been revealed, but the word 'ASTRA' is a Sanskrit word for 'weapon'.

Black Hat Hacker

Aug 24, 2023

OSI MODEL

Application	TELNET, SMTP, FTP, DNS
Presentation	
Session	

Transport	TCP, UDP
Network	IP, ARP, ICMP
Data Link	IEEE 802.2
Physical	Ethernet

Loopback address 127.0.0.1

PORTS

20, 21 FTP FILE TRANSFER PROTOCOL
Anonymous authentication (it’s possible to log into the FTP port with “anonymous” as the username and password)

22 SSH Secure SHELL
using leaked SSH keys or brute-forcing credentials.

23 TELNET
credential brute-forcing, spoofing and credential sniffing.

25 SMTP SIMPLE MAIL TRANSFER PROTOCOL
vulnerable to spoofing and spamming.

53 DNS DOMAIN NAME SERVER
This port is particularly vulnerable to DDoS attacks

69 TFTP TRIVIAL FILE TRANSFER PROTOCOL
TFTP does not have built-in encryption, access control or authentication. This makes it very easy for an attacker to trick TFTP into giving access to files.

80, 443 HTTP HTTPS
vulnerable to cross-site scripting, SQL injections, cross-site request forgeries and DDoS attacks.

110 POP3 (Post Office Protocol - Version 3)

Security Concerns: Re-usable cleartext password, no auditing of connections & attempts thus subject to grinding. Some POP3 server versions have had buffer overflow problems.
CERT Advisories: CA-97.09

123 NETWORK TIME PROTOCOL
Net Controller trojan

143 INTERNET MAIL ACCESS PROTOCOL

Numerous IMAP servers have buffer overflows that allow compromise during the login

MailServer.exe in NoticeWare Email Server 4.6.1.0 allows remote attackers to cause a denial of service (application crash) via a long string to IMAP port (143/tcp).

Aug 28, 2023

New web application vulnerabilities other than top10

Aug 29, 2023

Web Server vulnerabilities

Aug 30, 2023

Inventory of control over the hardware assets

20 heading

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs
Foundational
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and

Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls,
Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
Organizational
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Sep 4, 2023

NEssus website vulnerability