A team full of hackers

You scope it we pwn it

NORTHWAVE
CYBER SECURITY

Red team

What does PWN mean

"PWN" is a term that originated from gaming culture and is a leetspeak slang term derived from the word "own," meaning to appropriate or to conquer to gain ownership. The term implies domination or humiliation of a rival, typically in the gaming world. It's used to suggest that someone has been defeated or humiliated, often in a particularly impressive or thorough manner. For example, if a player defeats another player in a game, they might use the term "pwned" to assert their victory.

GO! lets start "Hacking"
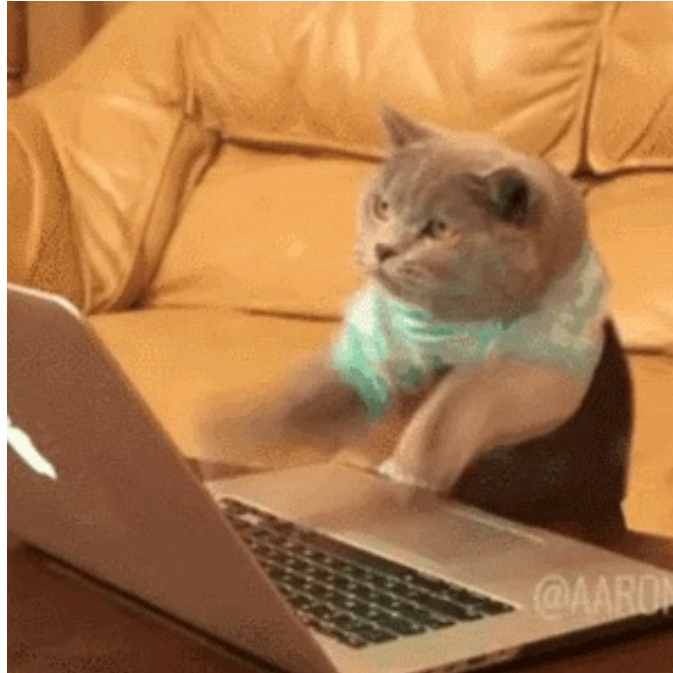
How does it work?

In

- Weaponisation
- Delivery & social engineering
- Exploitation
- Persistence
- Defense evasion
- Command & control

Through

- Discovery
- Privilege escalation
- Execution
- Credential access
- Lateral movement

Out

- Collection
- Exfiltration
- Impact
- Objectives

What is the best choice for a strong password?

a) 1ams0stron$

b) password12345

c) SummerAutumnWinterSummerSpringAutumn2023!

d) 9v4@x!3PQ$r2

e) 7h!5P@55w0rdIsReallyb@d&Anno1ng_

For a simple password (e.g., less than 8 characters, all lower case or common patterns), it could be seconds to minutes with powerful cracking tools and hardware.

For a complex password (e.g., 12 or more characters, with a mix of letters, numbers, and symbols), it could take from hundreds to millions of years with current technology, assuming that the attacker does not have a significant breakthrough in computing power, such as quantum computing.

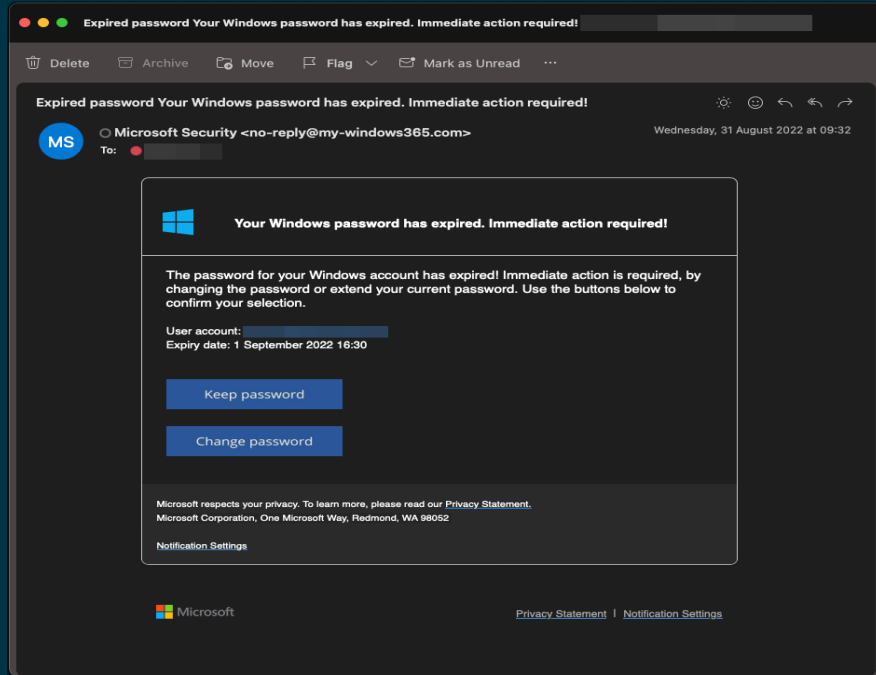~ > ./passwordspray.sh   at 16:35:20

What is a "zero-day exploit" in ethical hacking?

a) An exploit that targets vulnerabilities known for at least one day

b) An exploit that is not effective

c) An exploit that targets unknown vulnerabilities
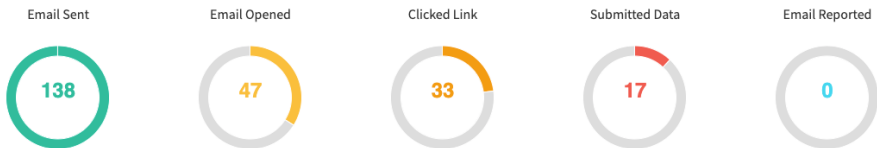
d) An exploit used on the zeroth day of an attack

5:00

We change it!

We don't.

Email Sent	Email Opened	Clicked Link	Submitted Data	Email Reported
138	47	33	17	0

Details

Show [10] entries

Search: [____]

▲ First Name	Last Name	Email	Position	Status	Reported
▼				Submitted Data	⊗

Timeline for ▮▮▮▮▮▮

Email: ▮▮▮▮▮▮
Result ID: VlGmnpW

🚀 **Campaign Created**   February 13th 2023 1:30:47 pm

✉ **Email Sent**   February 13th 2023 1:30:47 pm

🖱 **Clicked Link**   February 13th 2023 2:27:31 pm
   💻 Windows (OS Version: 10)
   🛡 Chrome (Version: 110.0.0.0)

❗ **Submitted Data**   February 13th 2023 2:28:03 pm
   💻 Windows (OS Version: 10)
   🛡 Chrome (Version: 110.0.0.0)

🔄 Replay Credentials

▼ View Details

Parameter	Value(s)
password	Zomer2020!
username	▮▮▮▮▮▮

What is the term for a fake network that is set up to intercept and collect data transmitted over a wireless network?

a) Firewall

b) VPN

c) Honeypot

d) Evil twin

In cybersecurity, a honeypot is a decoy system or network set up to attract cyber attackers.

The purpose of a honeypot is to detect, deflect, or study attempts at unauthorized use of information systems.

What is the difference between a red team and a penetration test?

a) Red teams are ethical hackers hired by organizations, while penetration tests involve in-house security teams.

b) Red teams are focused on finding and exploiting vulnerabilities, while penetration tests are aimed at assessing and identifying security weaknesses.

c) Red teams simulate external attackers, while penetration tests simulate internal network breaches

d) There is no significant difference; the terms "red team" and "penetration test" are interchangeable.

What is it called if a blue team works together with a red team after their hacking is done?

a) Gold teaming

b) Purple teaming

c) Yellow teaming

d) Collaboration overflow

Jaimy Thepass | LinkedIn

ThankYou

CLASSIFICATION TLP AMBER