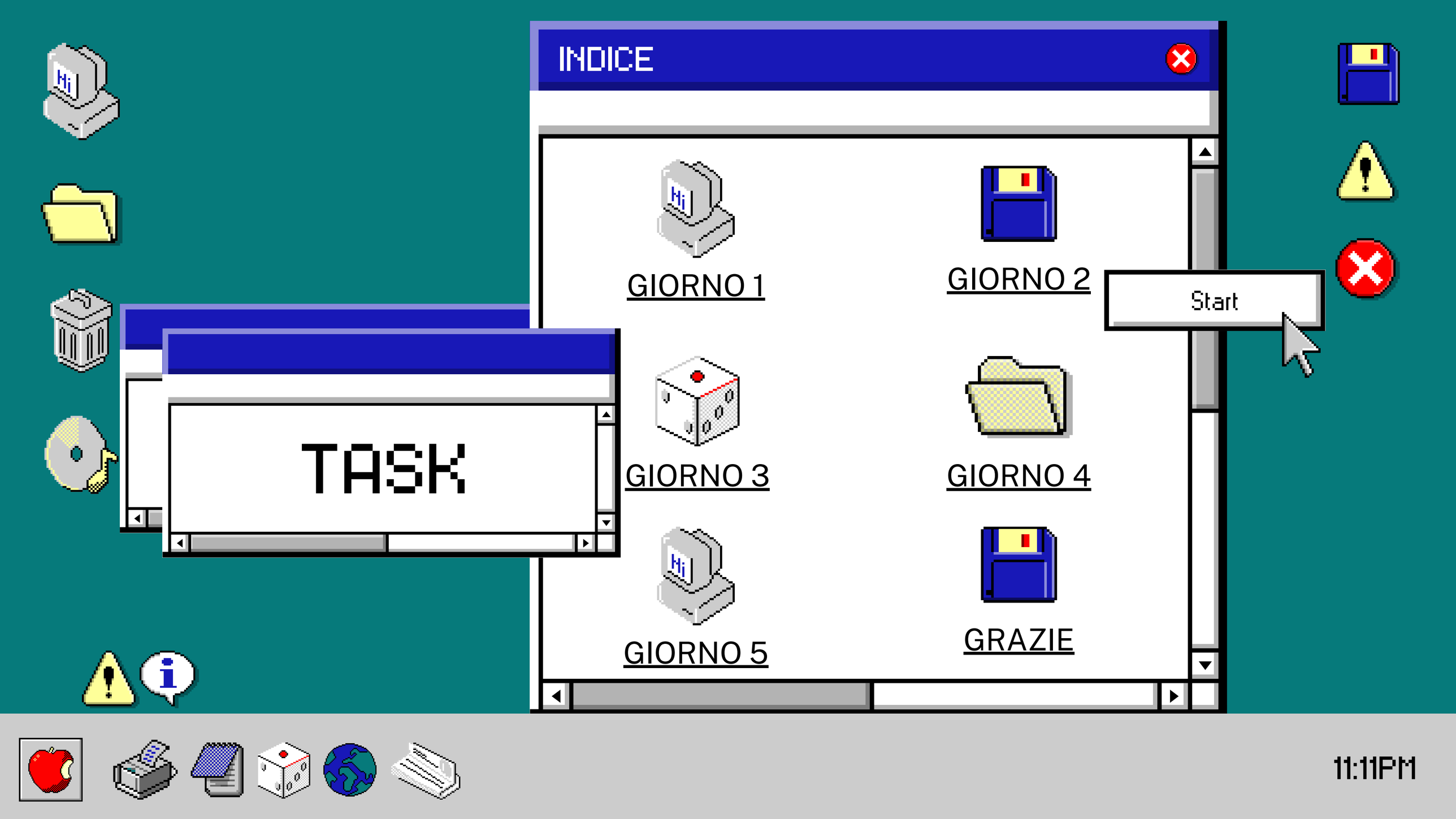
Build Week 2

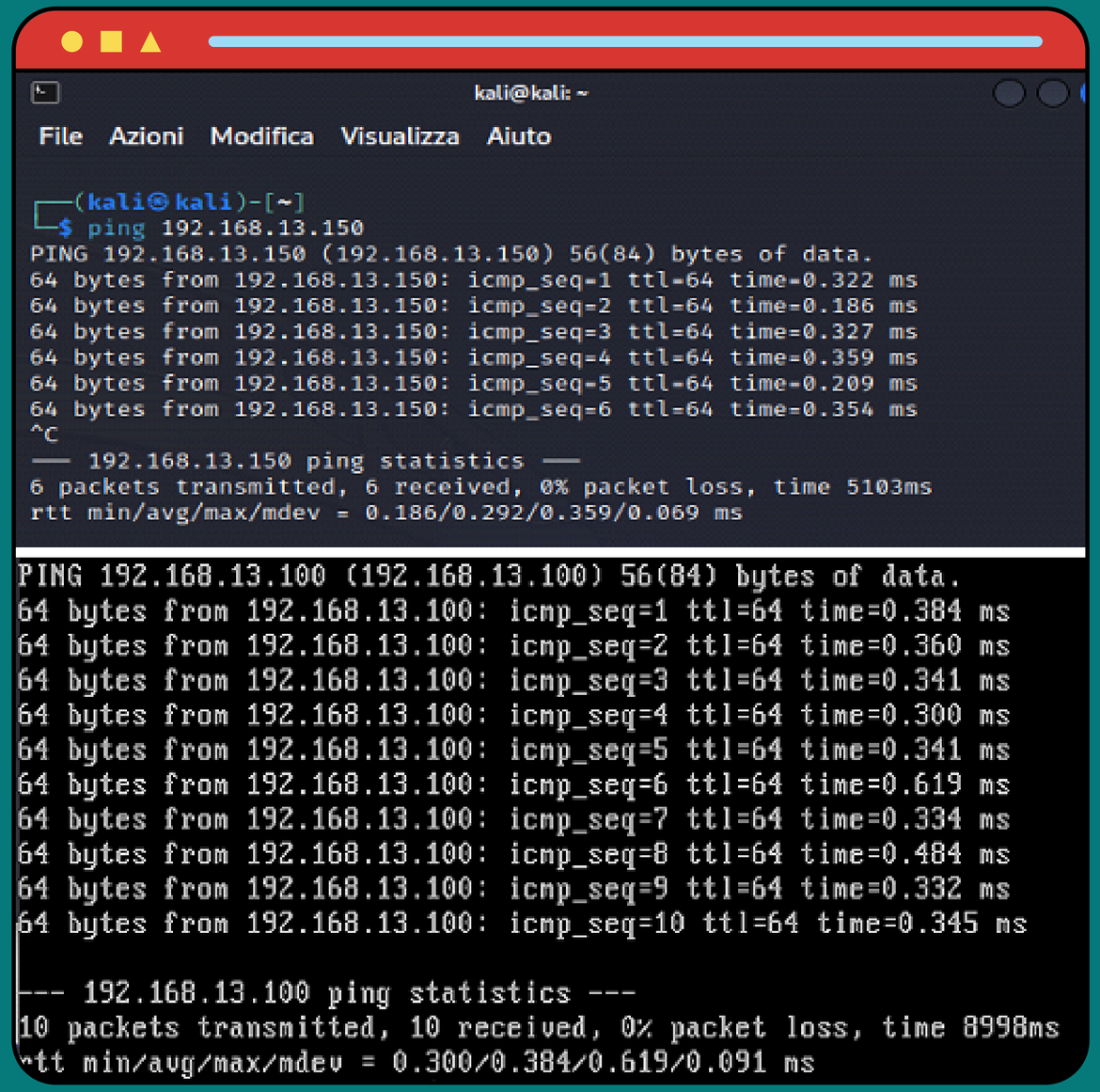
Mirabella, Di Mauro,
Kovalenko, Perelli,
Flores, Santigliano,
Rodrigues.

11:11PM

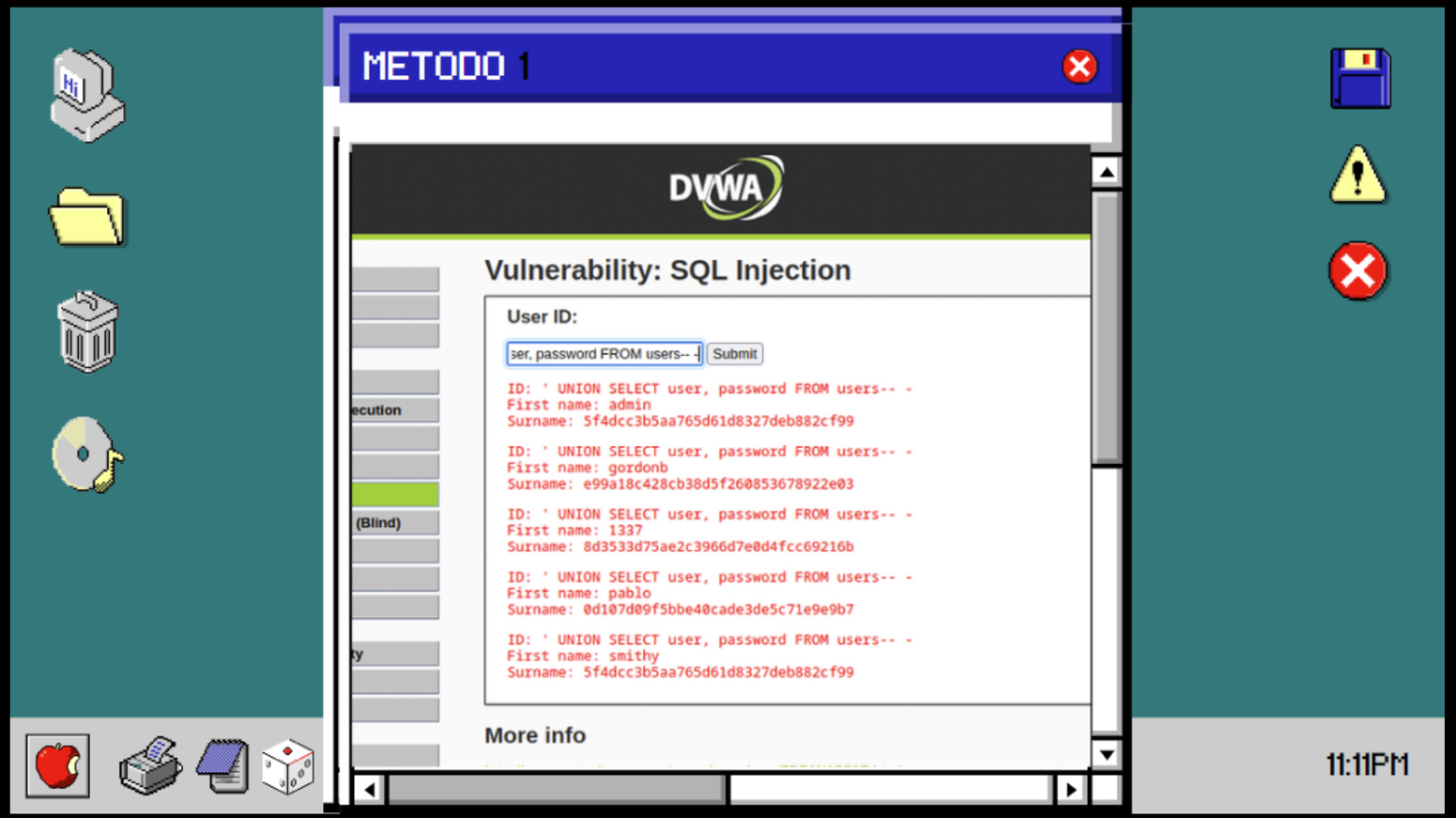

INDICE
GIORNO 1
GIORNO 2
GIORNO 3
GIORNO 4
GIORNO 5
GRAZIE
TASK
Start
11:11PM

GIORNO 1

CONFIGURIAMO IL LABORATORIO IMPOSTANDO I SEGUENTI REQUISITI:
L'INDIRIZZO IP DELLA MACCHINA KALI LINUX DEVE ESSERE 192.168.13.100/24;
L'INDIRIZZO IP DELLA MACCHINA METASPLOITABLE DEVE ESSERE 192.168.13.150/24;
IL LIVELLO DI DIFFICOLTA' DELLA APPLICAZIONE WEB DVWA DEVE ESSERE LOW.
GLI INDIRIZZI IP VENGONO CONFIGURATI ATTRAVERSO IL COMANDO:
SUDO NANO /ETC/NETWORK/INTERFACES.
IN QUESTO MODO, LA MACCHINA KALI LINUX E METASPLOITABLE SONO IN GRADO DI COMUNICARE FRA DI LORO.
EFFETTUIAMO UN TEST PER VEDERE SE CIO' AVVIENE ATTRAVERSO IL COMANDO PING.
ORA POSSO INIZIARE IL PROGETTO SULLA SQL INJECTION.



11:11PM



METODO 1

PER ESEGUIRE L'ESERCIZIO METTIAMO NELLA TAB SQL IL COMANDO:

'UNION SELECT USER, PASSWORD FROM USER-- -

IL DATABASE CI RESTITUIRA' GLI USERNAME E LE PASSWORD NELLA APPLICAZIONE WEB.

LE PASSWORD SONO CRITTOGRAFATE IN HASH.

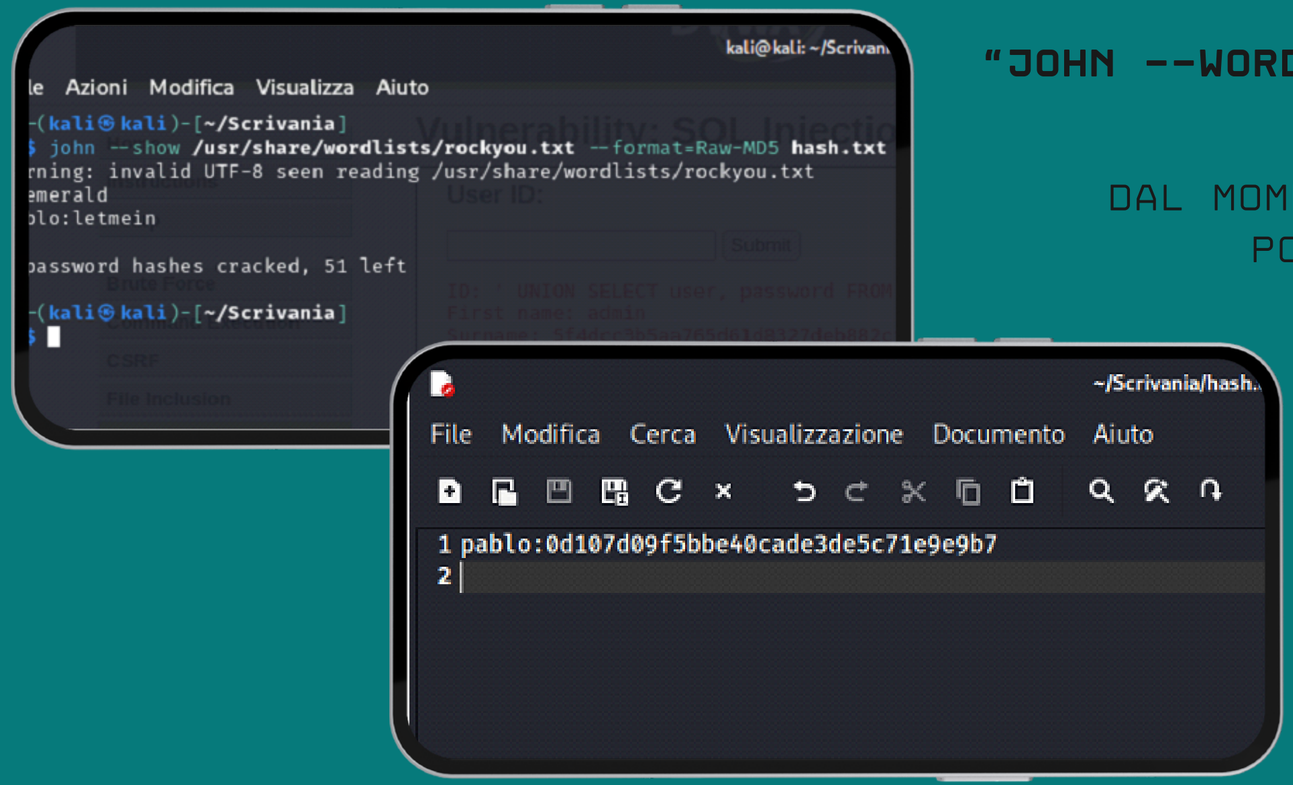
JOHN THE RIPPER

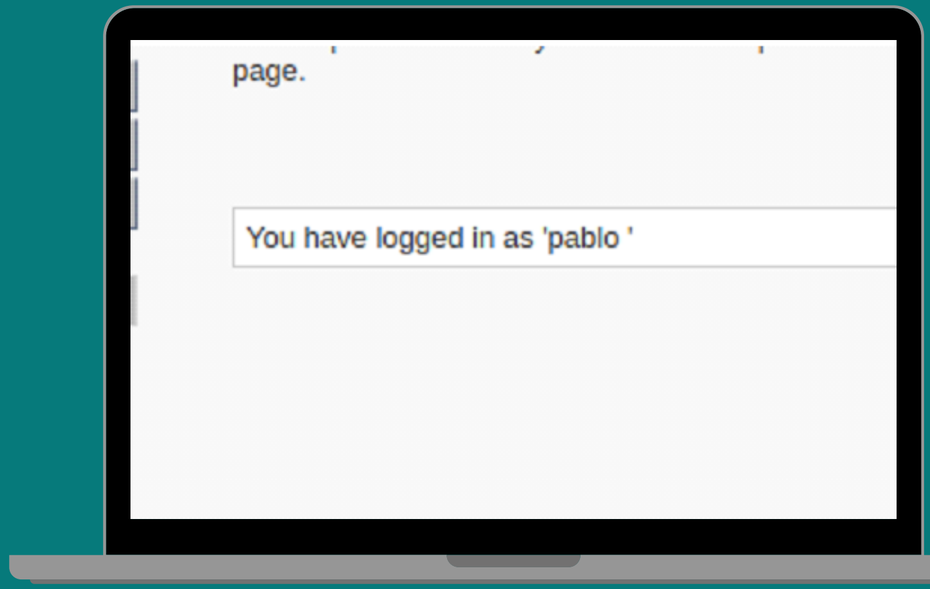
UTILIZIAMO JOHN THE RIPPER PER IL CRACKING DELLA PASSWORD.

INIZIAMO CREANDO UN FILE DI TESTO NELLA QUALE VIENE INSERITO I CODICI HASH TROVATI GRAZIE ALLA SQL INJECTION.
DOPODICHÉ LANCIAMO JTR UTILIZZANDO ROCKYOU.TXT CON IL COMANDO:

"JOHN --WORDLIST="/USR/SHARE/WORDLISTS/ROCKYOU.TXT" --FORMAT=RAW-MD5 HASH.TXT"

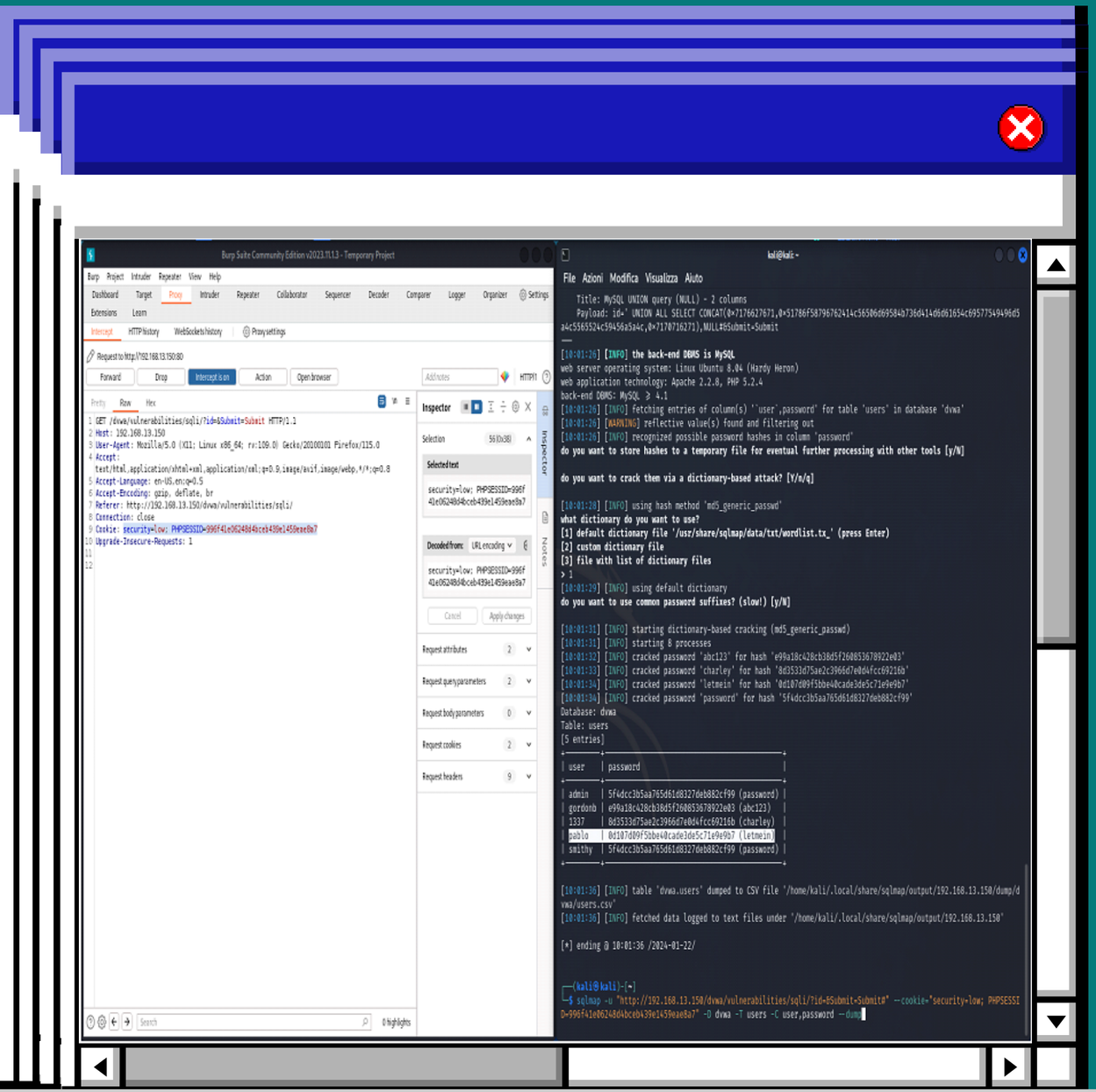
DAL MOMENTO CHE ABBIAMO SCOPERTO LA PASSWORD, POSSIAMO UTILIZZARLA PER ACCEDERE.





METODO 2

IL SECONDO METODO CONSISTE NELL'UTILIZZO DI BURPSUITE E SQLMAP. BURPSUITE CI FA RICAVARE I COOKIE DI SESSIONE E LO UTILIZZIAMO ACCEDENDO ALLA DVWA DAL BROWSER CHRONIUM E ATTIVANDO L'INTERCETTAZIONE.
RICAVANDO I COOKIE DI SESSIONE, LANCIAMO SQL. POICHÉ IL PARAMETRO ID È VULNERABILE POSSIAMO SFRUTTARE IL TOOL PER EFFETTUARE UN ATTACCO A DIZIONARIO PER TROVARE LE PASSWORD IN CHIARO.



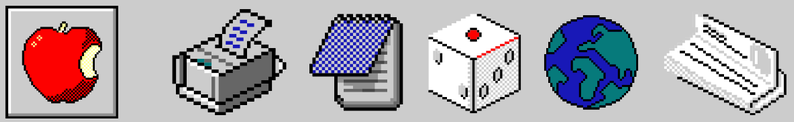
11:13PM

CONCLUSIONI

SERIA MINACCIA PER LA SICUREZZA: GLI ATTACCHI DI SQL INJECTION RAPPRESENTANO UNA MINACCIA SIGNIFICATIVA PER LA SICUREZZA DELLE APPLICAZIONI WEB. SFRUTTANDO VULNERABILITÀ NEL CODICE SQL DI UN'APPLICAZIONE, GLI ATTACCANTI POSSONO COMPROMETTERE LA RISERVATEZZA, L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI.

POTENZIALI IMPATTI: GLI IMPATTI DI UN ATTACCO DI SQL INJECTION POSSONO VARIARE DAL RECUPERO NON AUTORIZZATO DI DATI SENSIBILI, ALL'ALTERAZIONE DEI DATI NEL DATABASE, FINO ALLA DISTRUZIONE DEI DATI STESSI.

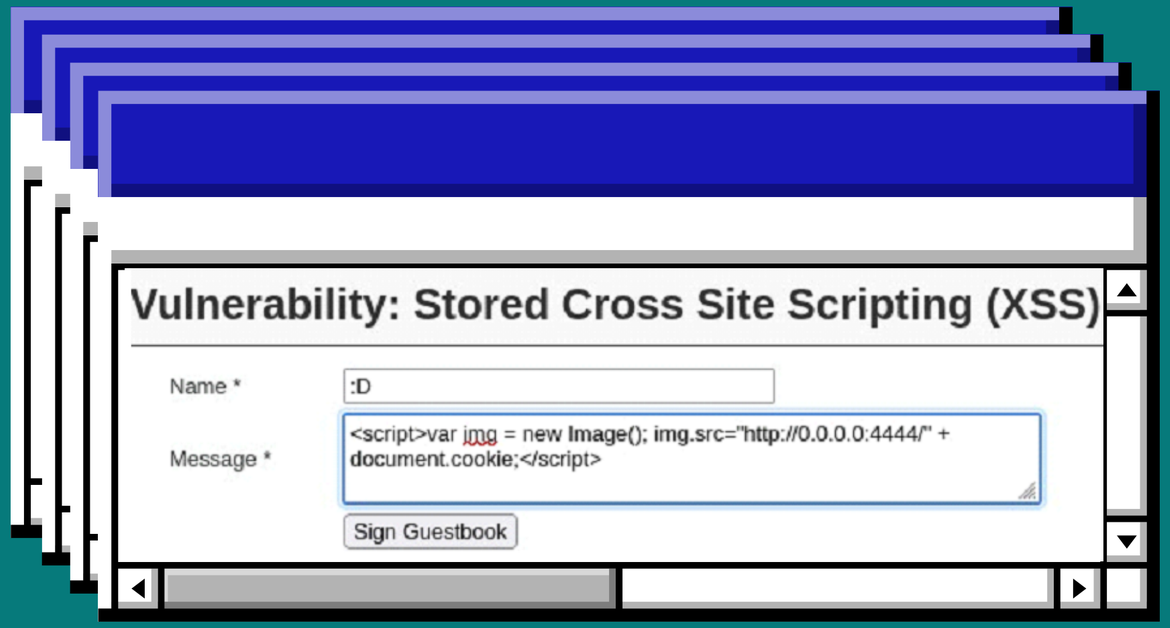
RISCHI PER LA REPUTAZIONE: LE VIOLAZIONI DELLA SICUREZZA DOVUTE A SQL INJECTION POSSONO DANNEGGIARE GRAVEMENTE LA REPUTAZIONE DI UN'ORGANIZZAZIONE. LA PERDITA DI DATI SENSIBILI PUÒ AVERE CONSEGUENZE FINANZIARIE E LEGALI SIGNIFICATIVE, OLTRE A ERODERE LA FIDUCIA DEGLI UTENTI.



11:13PM

GIORNO 2

INIZIAMO CON LA CONFIGURAZIONE DELLE MACCHINE VIRTUALI COME FATTO IN PRECEDENZA.



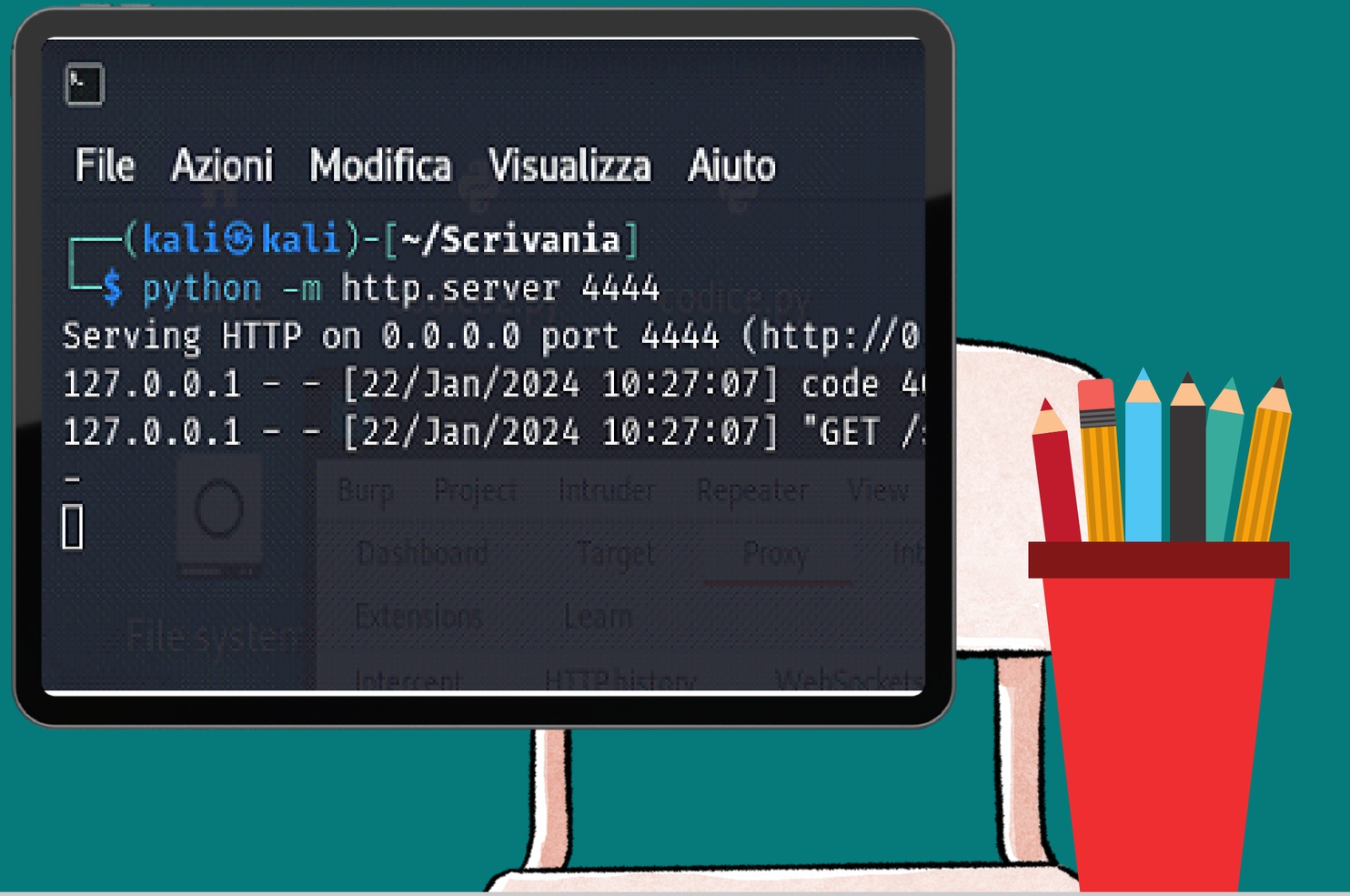
L'OBIETTIVO DI QUESTO ESERCIZIO È SFRUTTARE LE VULNERABILITÀ XSS PRESENTE SULLA APPLICAZIONE WEB CON LO SCOPO DI SIMULARE IL FURTO DI UNA SESSIONE DI UN UTENTE DEL SITO E
INOLTRARE I COOKIE SU UN SERVER IN ASCOLTO CREATO IN PRECEDENZA.

I COOKIE DOVRANNO ESSERE RICEVUTI SU UN WEB SERVER IN ASCOLTO SULLA PORTA 4444.

NELLA SEZIONE XSS STORED DELLA PAGINA DVWA INSERIAMO LO SCRIPT CHE CREA UN TAG IMG CHE HA COME PERCORSO DELL'IMMAGINE L'INDIRIZZO IP DEL NOSTRO SERVER WEB.

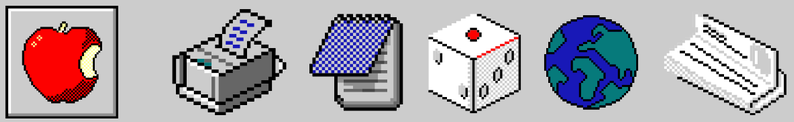
11:14PM

TRAMITE QUESTO SCRIPT È POSSIBILE RICAVARE I COOKIE DI SESSIONE E INVIARLI A UN SERVER IN ASCOLTO SULLA PORTA 4444.



CONCLUSIONI

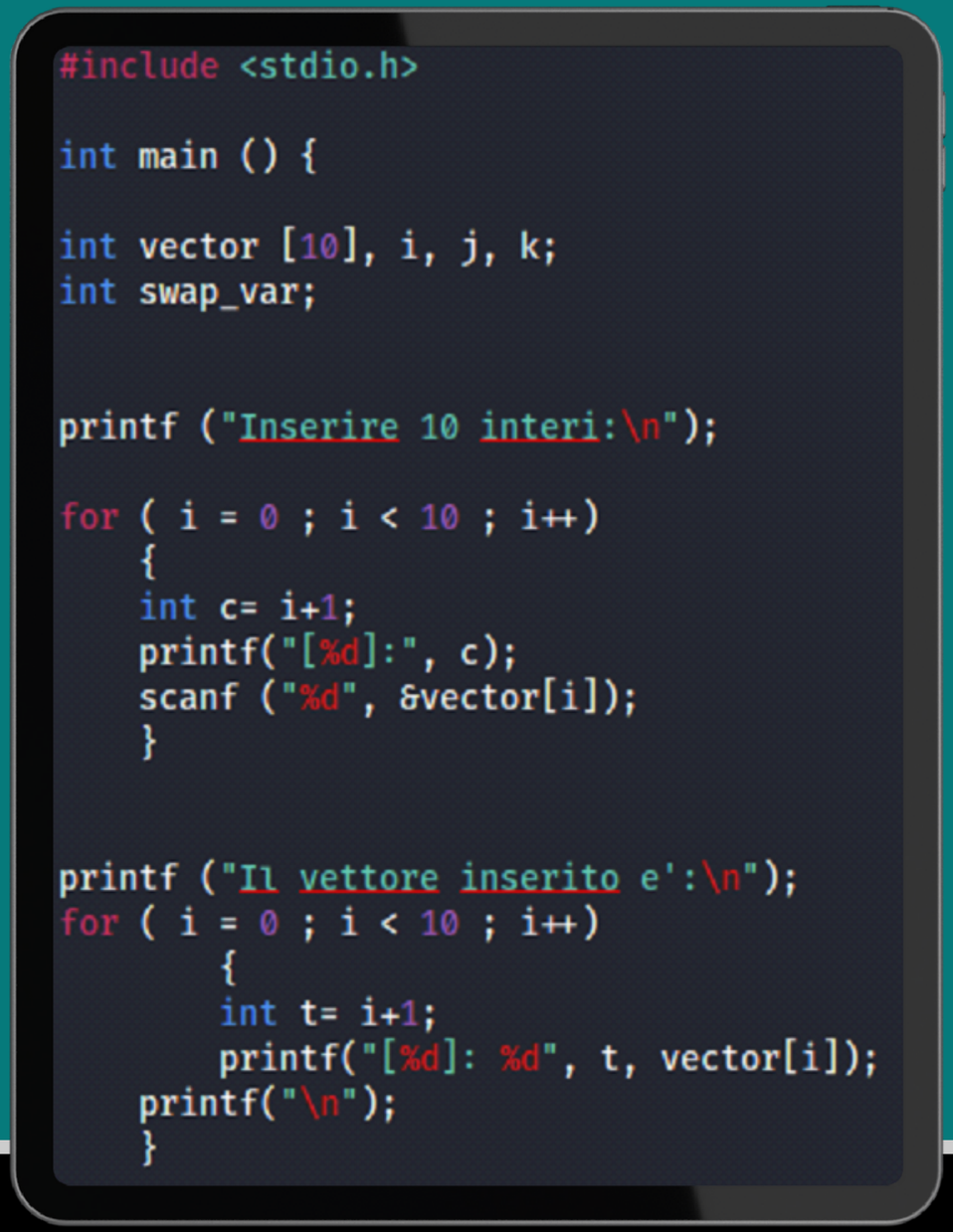
XSS STORED RAPPRESENTA UNA MINACCIA PER LA SICUREZZA DELLE WEB APPLICATION, POICHÉ CONSENTE AGLI ATTACCANTI DI INSERIRE SCRIPT MALEVOLI E MEMORIZZARLI SUI SERVER BACKEND CREANDO DANNI AGLI UTENTI. L'USO DI LIBRERIE SICURE E AGGIORNATE ED UNA CORRETTA SANIFICAZIONE DEI DATI IN INPUT POSSONO CONTRIBUIRE A DIMINUIRE I RISCHI ASSOCIATI A QUESTA VULNERABILITÀ.



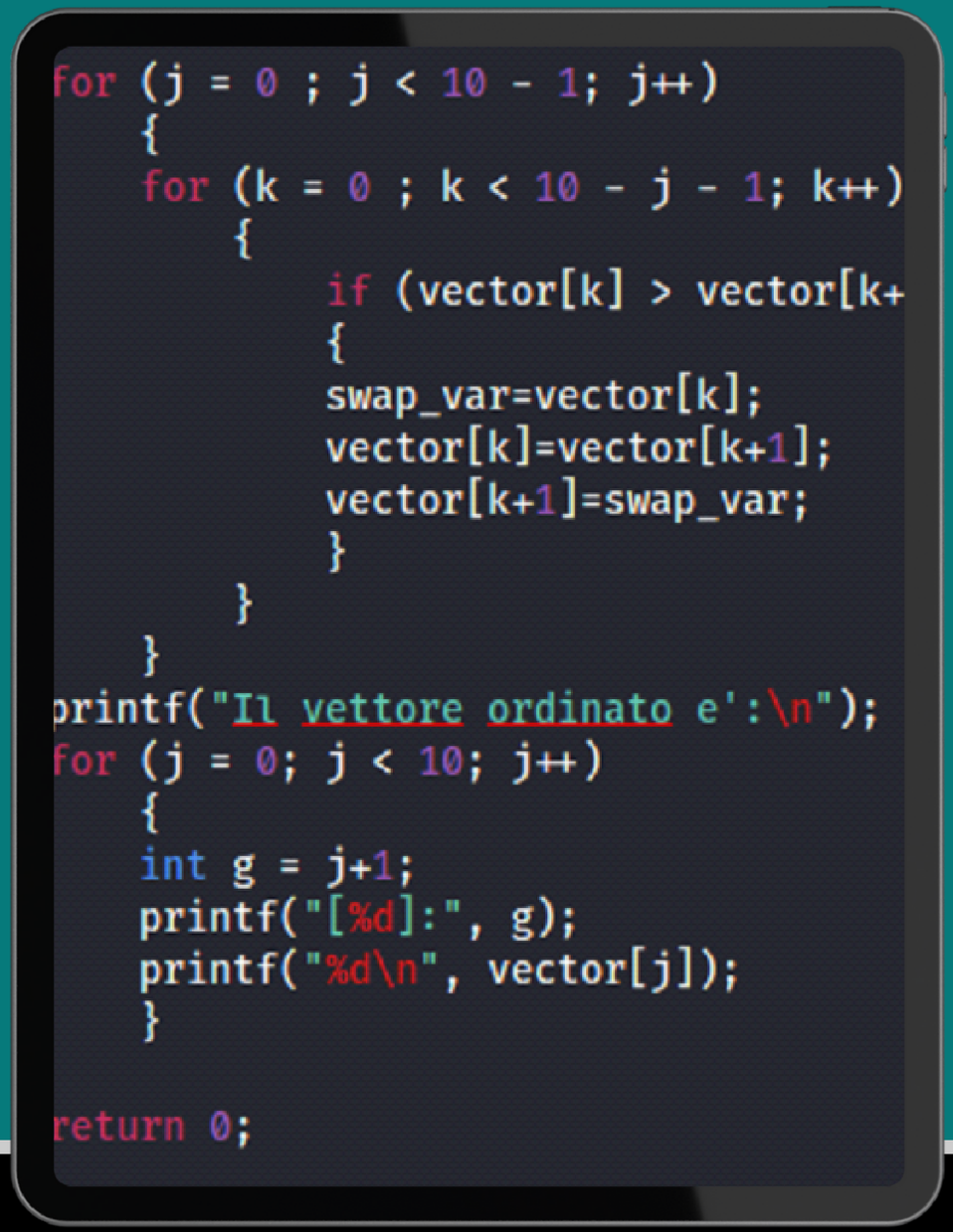
```
Inserire 10 interi:
[1]:1
[2]:2
[3]:3
[4]:4
[5]:5
[6]:6
[7]:7
[8]:8
[9]:9
[10]:10
Il vettore inserito e':
[1]: 1
[2]: 2
[3]: 3
[4]: 4
[5]: 5
[6]: 6
[7]: 7
[8]: 8
[9]: 9
[10]: 10
```

GIORNO 3

NELL'ESERCIZIO DEL GIORNO 3 DOVREMO EFFETTUARE LE SEGUENTI OPERAZIONI: DESCRIVERE IL FUNZIONAMENTO DI UN BUFFER OVERFLOW PRIMA CHE VENGA ESEGUITO E MODIFICARLO CON LO SCOPO CHE SI VERIFICHI UN ERRORE DI SEGMENTAZIONE.



```c
#include <stdio.h>

int main () {

int vector [10], i, j, k;
int swap_var;


printf ("Inserire 10 interi:\n");

for ( i = 0 ; i < 10 ; i++)
    {
    int c= i+1;
    printf("[%d]:", c);
    scanf ("%d", &vector[i]);
    }


printf ("Il vettore inserito e':\n");
for ( i = 0 ; i < 10 ; i++)
        {
        int t= i+1;
        printf("[%d]: %d", t, vector[i]);
    printf("\n");
    }
```



```c
for (j = 0 ; j < 10 - 1; j++)
    {
    for (k = 0 ; k < 10 - j - 1; k++)
        {
            if (vector[k] > vector[k+
            {
            swap_var=vector[k];
            vector[k]=vector[k+1];
            vector[k+1]=swap_var;
            }
        }
    }
printf("Il vettore ordinato e':\n");
for (j = 0; j < 10; j++)
    {
    int g = j+1;
    printf("[%d]:", g);
    printf("%d\n", vector[j]);
    }

return 0;
```

IL PROGRAMMA È STATO CREATO AFFINCHÉ RICHIEDA ALL'UTENTE DI INSERIRE 10 NUMERI INTERI PER POTERLI ORDINARE IN ORDINE CRESCENTE.

PROGRAMMA MODIFICATO

```c
#include <stdio.h>
#include <stdbool.h>

int main() {
    int f;
    printf("Inserisci 10 numeri interi \n");
    printf("Inserire il numero 1414 per uscire dal p

    int vector[10 + f], i, j, k;
    int swap_var;
    bool esciDalProgramma = false;

    for (i = 0; i < 25; i++) {
        int c = i + 1;
        printf("[%d]:", c);
        scanf("%d", &vector[i]);

        if (vector[i] == 1414) {
            esciDalProgramma = true;
            break;
        }

        if (i == 9) {
            char risposta;
            printf("Vuoi inserire altri parametri? (
            scanf(" %c", &risposta);

            if (risposta != 's' && risposta != 'S')
                printf("Inserimento annullato.\n");
                break;
            }
        }
    }
```

```c
    if (!esciDalProgramma) {
        printf("Il vettore inserito e':\n");
        for (i = 0; i < 25; i++) {
            int t = i + 1;
            printf("[%d]: %d\n", t, vector[i]);
        }

        for (j = 10; j < 10 + f - 1; j++) {
            for (k = 10; k < 10 + f - j - 1; k++) {
                if (vector[k] > vector[k + 1]) {
                    swap_var = vector[k];
                    vector[k] = vector[k + 1];
                    vector[k + 1] = swap_var;
                }
            }
        }

        printf("La parte del vettore ordinato e':\n")
        for (j = 10; j < 10 + f; j++) {
            int g = j + 1;
            printf("[%d]: %d\n", g, vector[j]);
        }
    } else {
        printf("Uscita dal programma: l'utente ha ins
    }

    return 0;
}
```

ESSO RICHIEDE ALL'UTENTE DI INSERIRE 10 NUMERI INTERI OPPURE DI TERMINARE L'ESECUZIONE DEL PROGRAMMA INSERENDO IL NUMERO 1414.

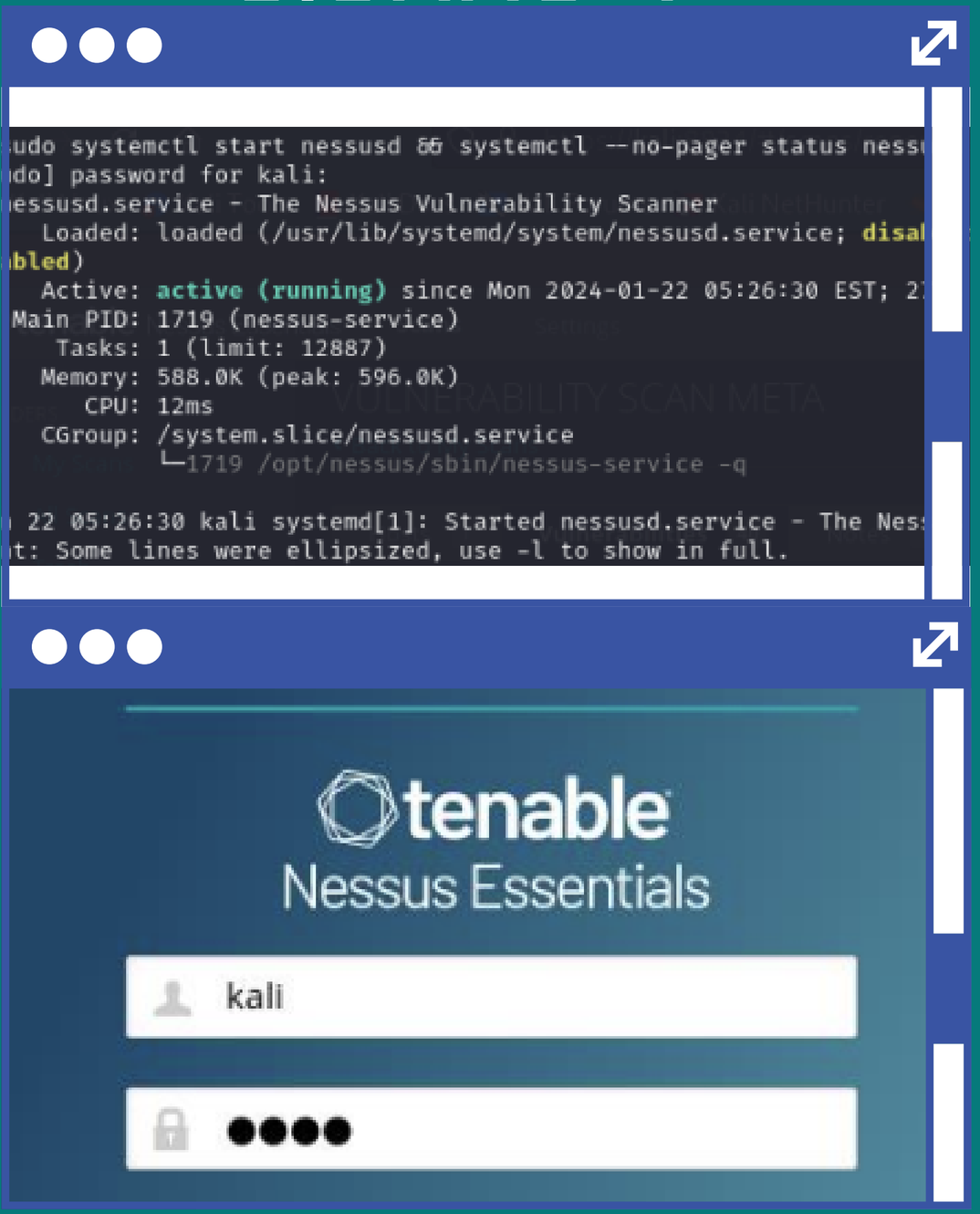
ALLA FINE DELL'INSERIMENTO DEI 10 NUMERI RICHIESTI, IL PROGRAMMA LASCIA ALL'UTENTE L'OPZIONE DI AGGIUNGERE ULTERIORI PARAMETRI.

ALL'AGGIUNTA DI ULTERIORI PARAMETRI DA PARTE DELL'UTENTE NEL PROGRAMMA SI CREA UN PROBLEMA DI SEGMENTAZIONE.

CONCLUSIONI

IL PRIMO PROGRAMMA CHIEDE ALL'UTENTE DI INSERIRE 10 NUMERI, LI ORDINA E LI STAMPA IN MODO CRESCENTE. IL SECONDO PROGRAMMA È STATO MODIFICATO PER CONSENTIRE L'INSERIMENTO DI PIÙ DI 10 NUMERI, OFFRENDO LA POSSIBILITÀ DI USCIRE INSERENDO IL NUMERO "1414". TUTTAVIA, PRESENTA UN RISCHIO DI ERRORE DI SEGMENTAZIONE POICHÉ NON CONTROLLA ADEGUATAMENTE LA DIMENSIONE DELL'ARRAY QUANDO L'UTENTE INSERISCE PIÙ NUMERI. QUESTO PUÒ CAUSARE UN PROBLEMA DURANTE L'ORDINAMENTO DEL VETTORE OLTRE LA SUA DIMENSIONE ALLOCATA. È IMPORTANTE IMPLEMENTARE CONTROLLI APPROPRIATI PER EVITARE ERRORI DI SEGMENTAZIONE NELLA GESTIONE DELLA MEMORIA.

GIORNO 4



NELL'ESERCIZIO DEL GIORNO 4 SI RICHIEDE DI:

- EFFETTURARE UN BASIC SCAN CON NESSUS SULLA MACCHINA META;
- SFRUTTARE LA VULNERABILITÀ DEL SERVIZIO ATTIVO SULLA PORTA 445 TCP UTILIZZANDO MSFCONSOLE;
- ESEGUIRE IL COMANDO "IFCONFIG" PER VERIFICARE L'INDIRIZZO DI RETE DELLA MACCHINA VITTIMA.

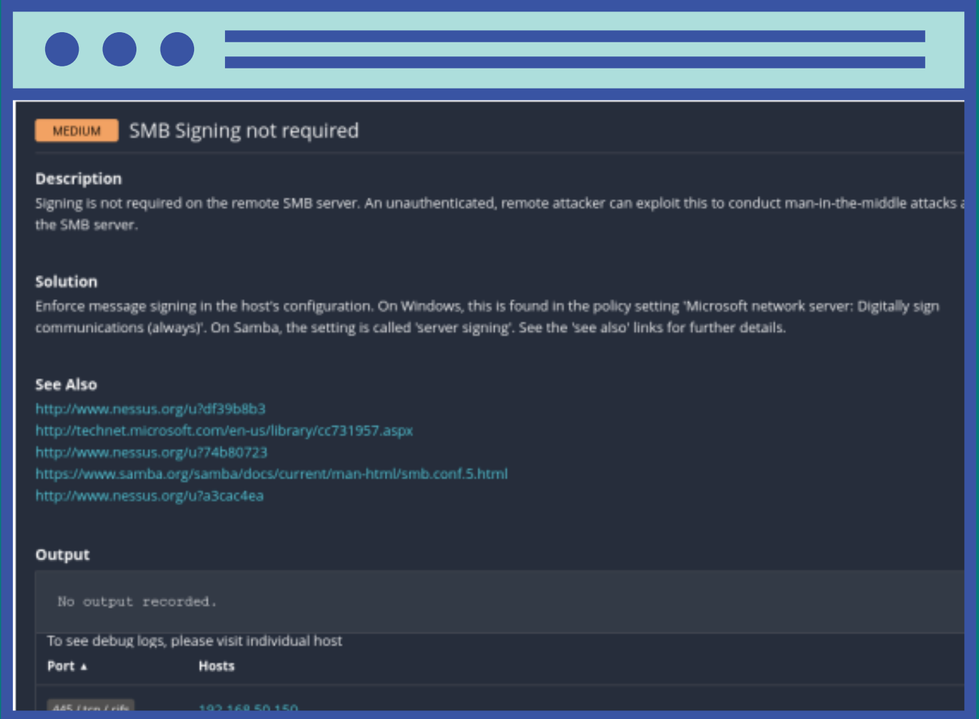
ABBIAMO GIÀ CONFIGURATO IL LABORATORIO COME ESEGUITO IN PRECEDENZA.

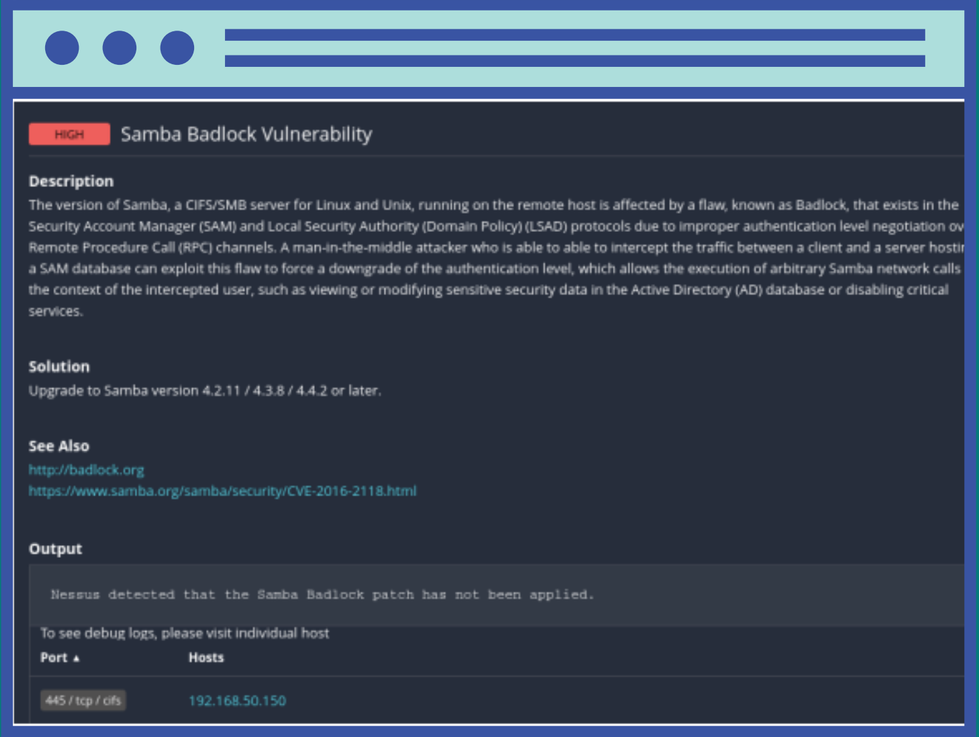
FACCIAMO PARTIRE NESSUS E, DOPO ESSERE ENTRATI SULLA PAGINA WEB DI NESSUS, AVVIAMO LA SCANSIONE.

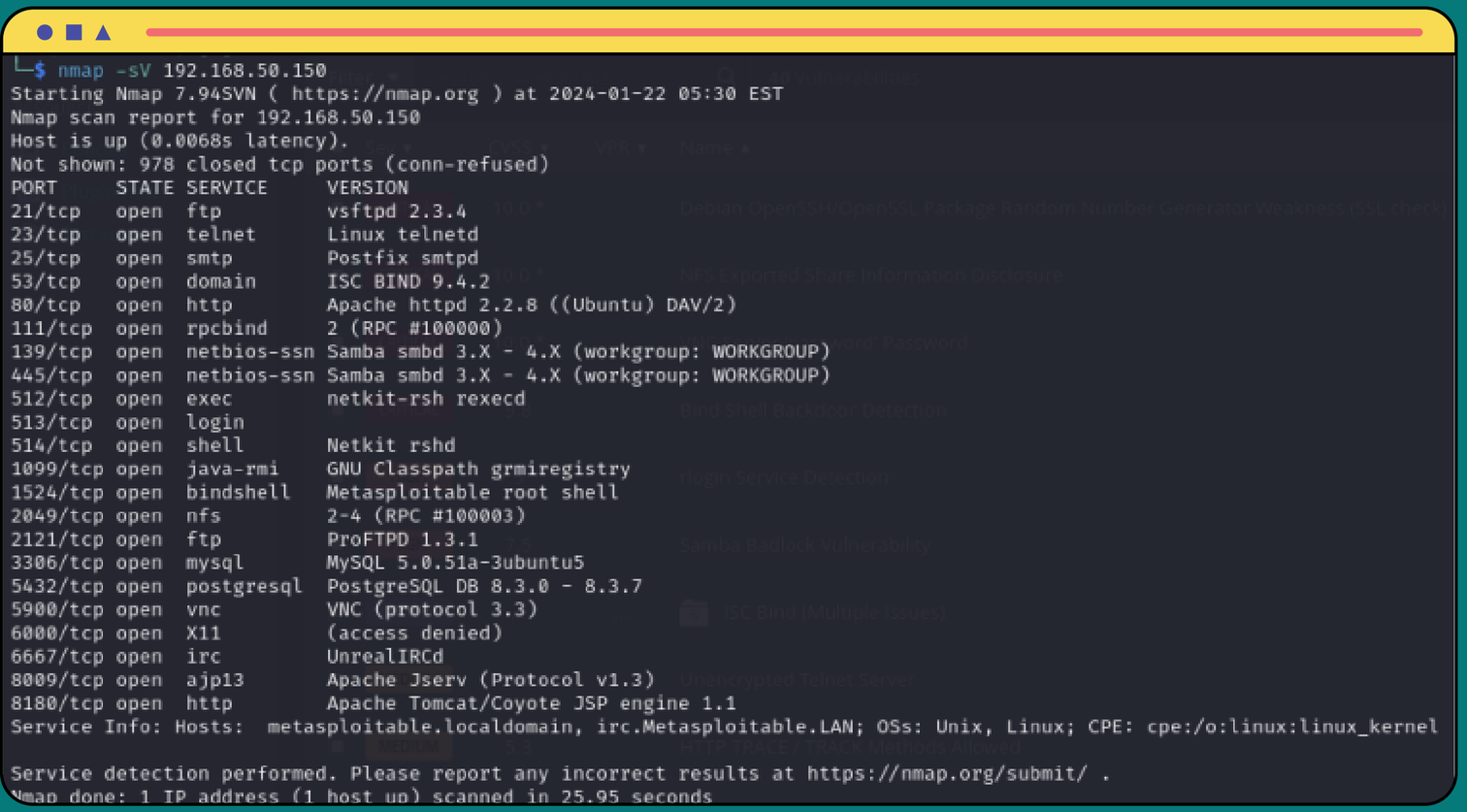
VULNERABILITA' TROVATE

SONO STATE TROVATE DUE VULNERABILITA':

- IL PLUGIN 57608:ESSO TENTA UN ACCESSO SMB.
  DURANTE IL LOGIN VERIFICA I REQUISITI PER LA FIRMA SMB.
- SAMBA BADCLOCK VULNERABILITY:
  ESSA È UNA FALLA CHE COINVOLGE I PROTOCOLLI SAM E LSAD A CAUSA DI UNA NEGOZIAZIONE NON CORRETTA DEL LIVELLO DI AUTENTICAZIONE SU CANALI RPC.



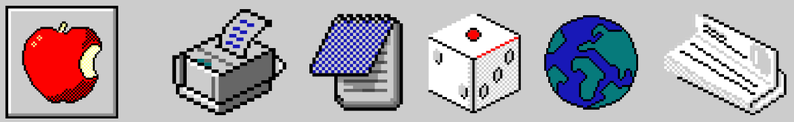




```
└─$ nmap -sV 192.168.50.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 05:30 EST
Nmap scan report for 192.168.50.150
Host is up (0.0068s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.95 seconds
```

UTILIZZIAMO LA SCANSIONE NMAP SULLA MACCHINA METASPLOITABLE CHE CI RESTTUISCE I SERVIZI APERTI SULLE PORTE 139/TCP E 445/TCP.

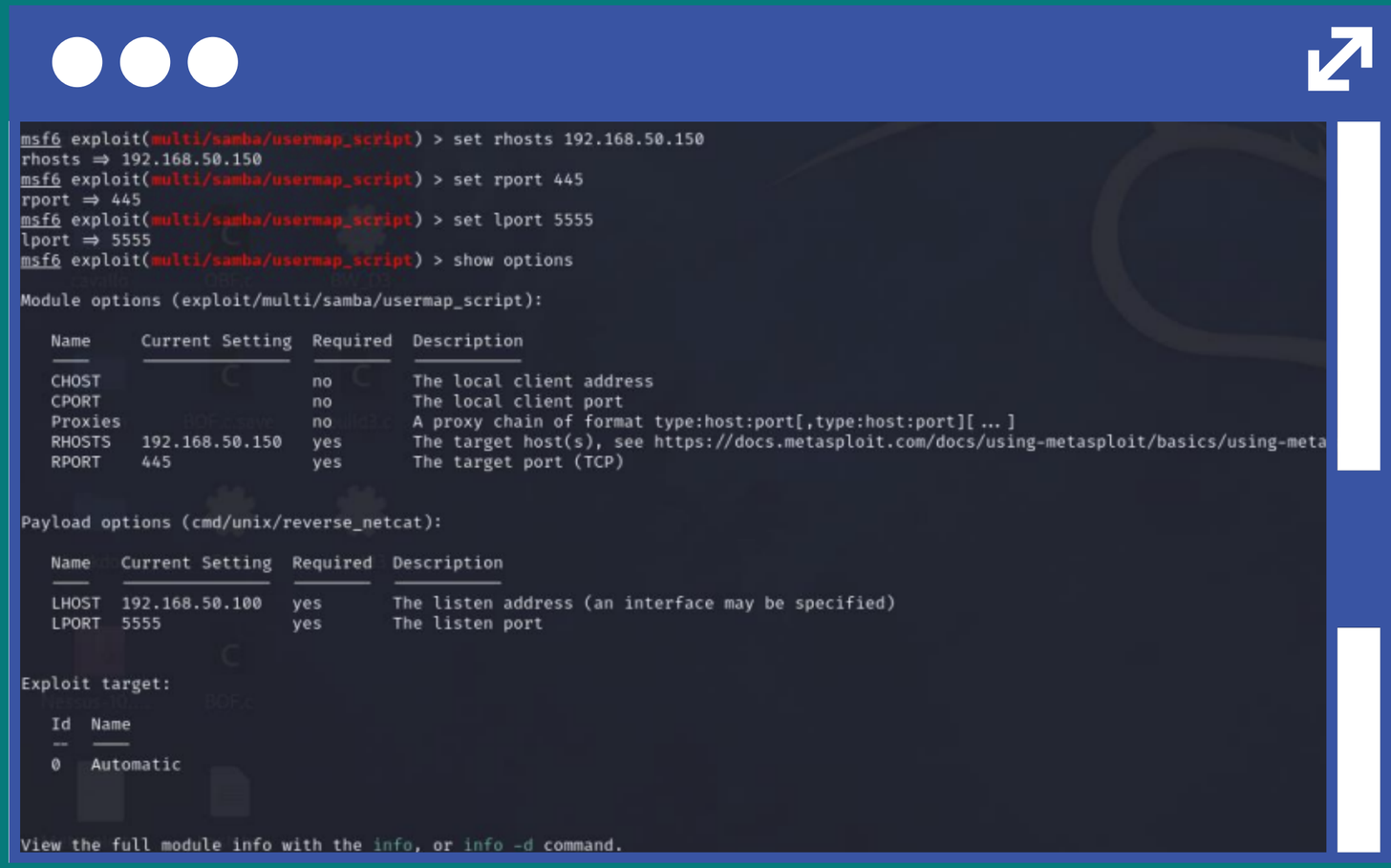
PERTANTO, ORA POSSIAMO PROCEDERE PER CERCARE DI EFFETTUARE UN ATTACCO E OTTENERE UNA SESSIONE SULLA MACCHINA TARGET DI META.



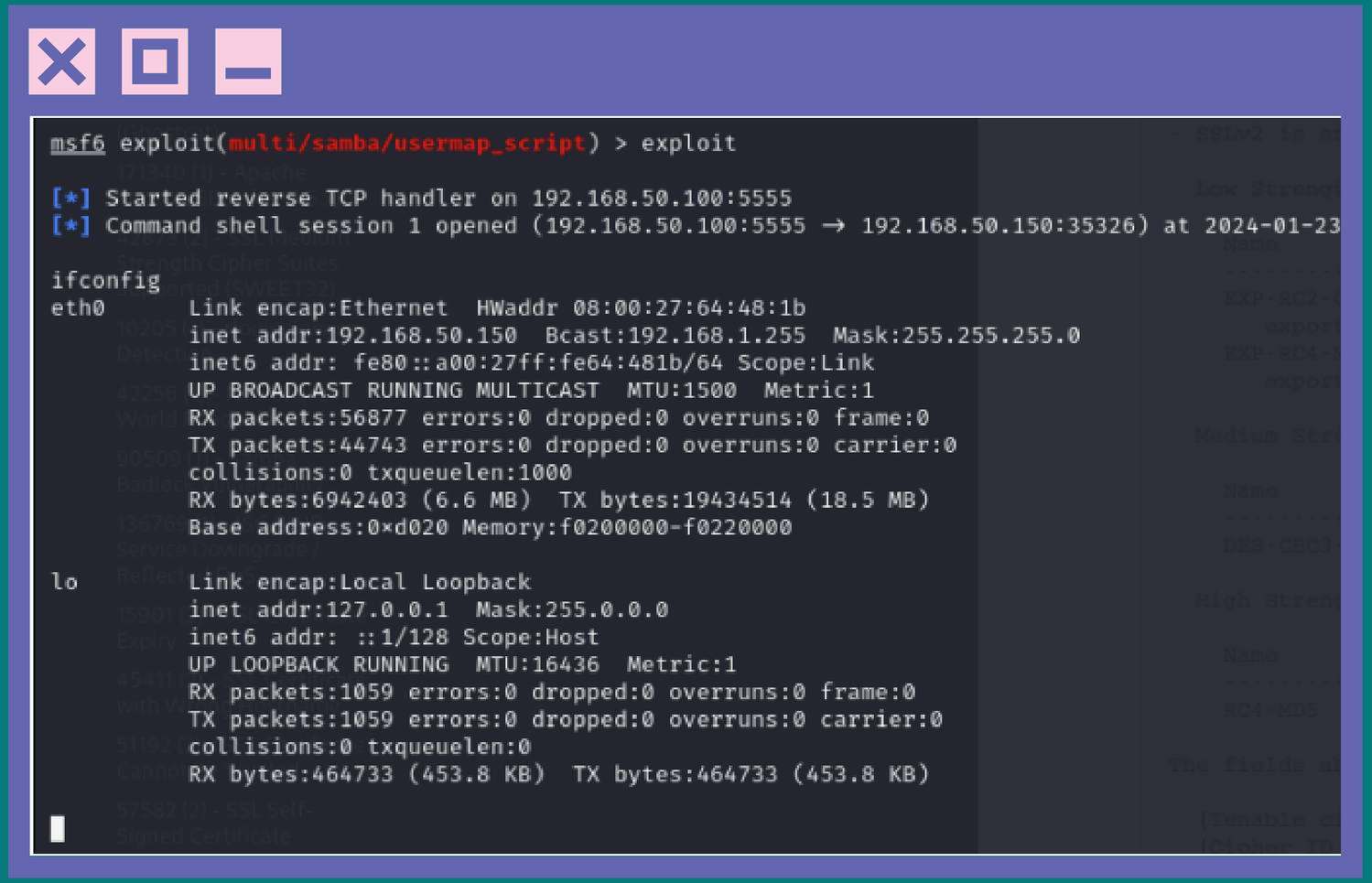
11:16PM

SFRUTTIAMO LE VULNERABILITÀ TROVATE IN PRECEDENZA CON METASPLOIT.

UTILIZZANDO LO SCRIPT CHE VIENE SUGGERITO NELLA TRACCIA, CONFIGURIAMO L'INDIRIZZO IP DELLA MACCHINA TARGET, LA PORTA DELLA MACCHINA TARGET 445 E LA PORTA IN ASCOLTO SULLA NOSTRA MACCHINA 5555.



11:16PM

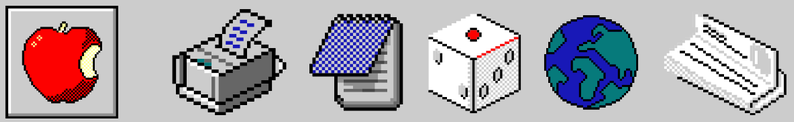


ORA CHE LA SESSIONE È STATA OTTENUTA POSSIAMO ESEGUIRE IL COMANDO IFCONFIG COME RICHIESTO DALLA TRACCIA.

11:17PM

CONCLUSIONI

DURANTE LA QUARTA GIORNATA, ABBIAMO ESEGUITO UNA SCANSIONE DI VULNERABILITÀ SULLA MACCHINA META UTILIZZANDO NESSUS, IDENTIFICANDO CRITICITÀ NEL SERVIZIO SMB SULLA PORTA TCP 445. SUCCESSIVAMENTE, CON NMAP, ABBIAMO CONFERMATO LE PORTE E I SERVIZI ATTIVI. UTILIZZANDO METASPLOIT E UNO SPECIFICO SCRIPT SMB, ABBIAMO SFRUTTATO LE VULNERABILITÀ PER OTTENERE ACCESSO REMOTO A META. INFINE, ABBIAMO VERIFICATO L'INDIRIZZO DI RETE DI META TRAMITE IL COMANDO "IFCONFIG". L'APPROCCIO HA DIMOSTRATO L'IMPORTANZA DELLA VALUTAZIONE CONTINUA DELLA SICUREZZA.



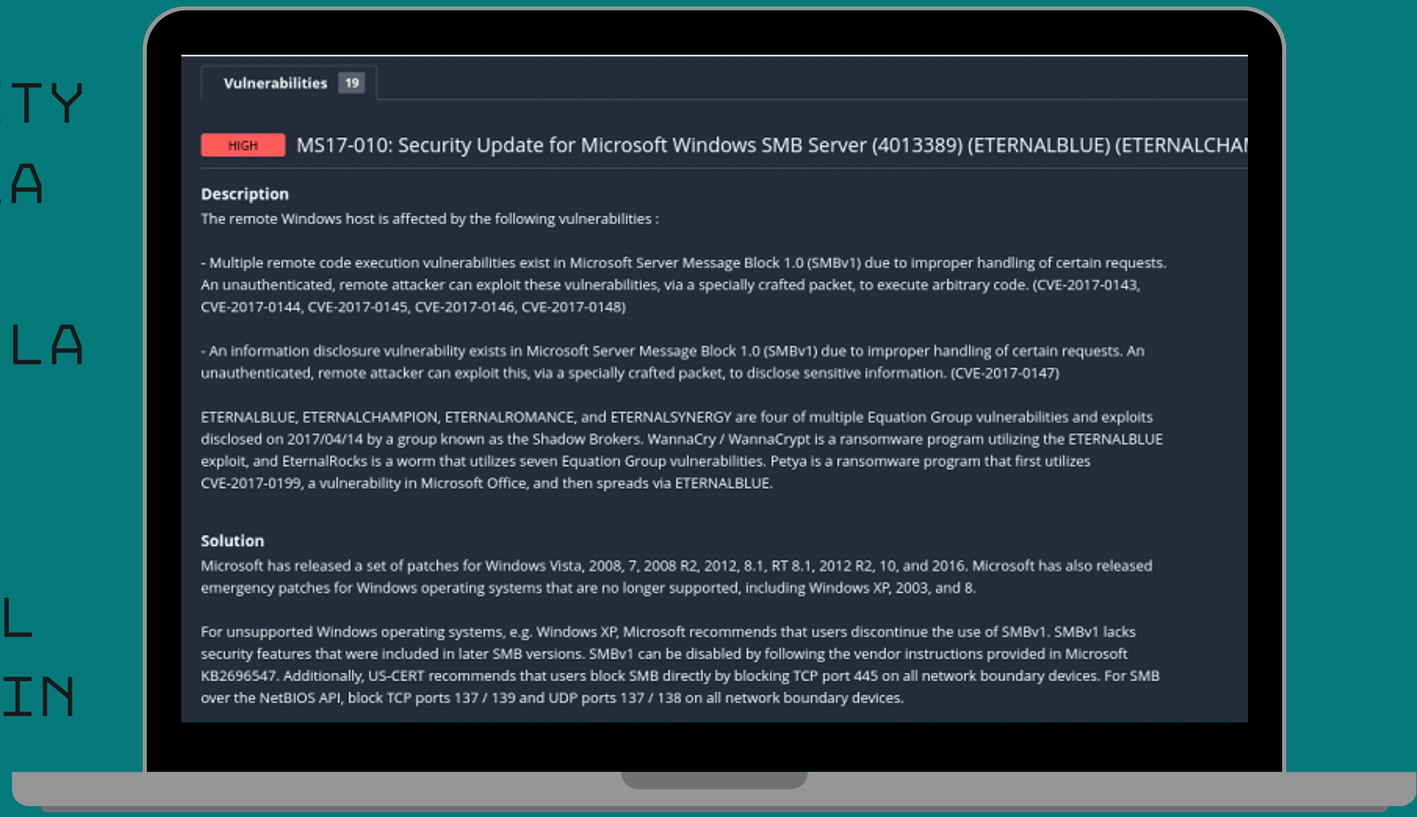
11:17PM

GIORNO 5

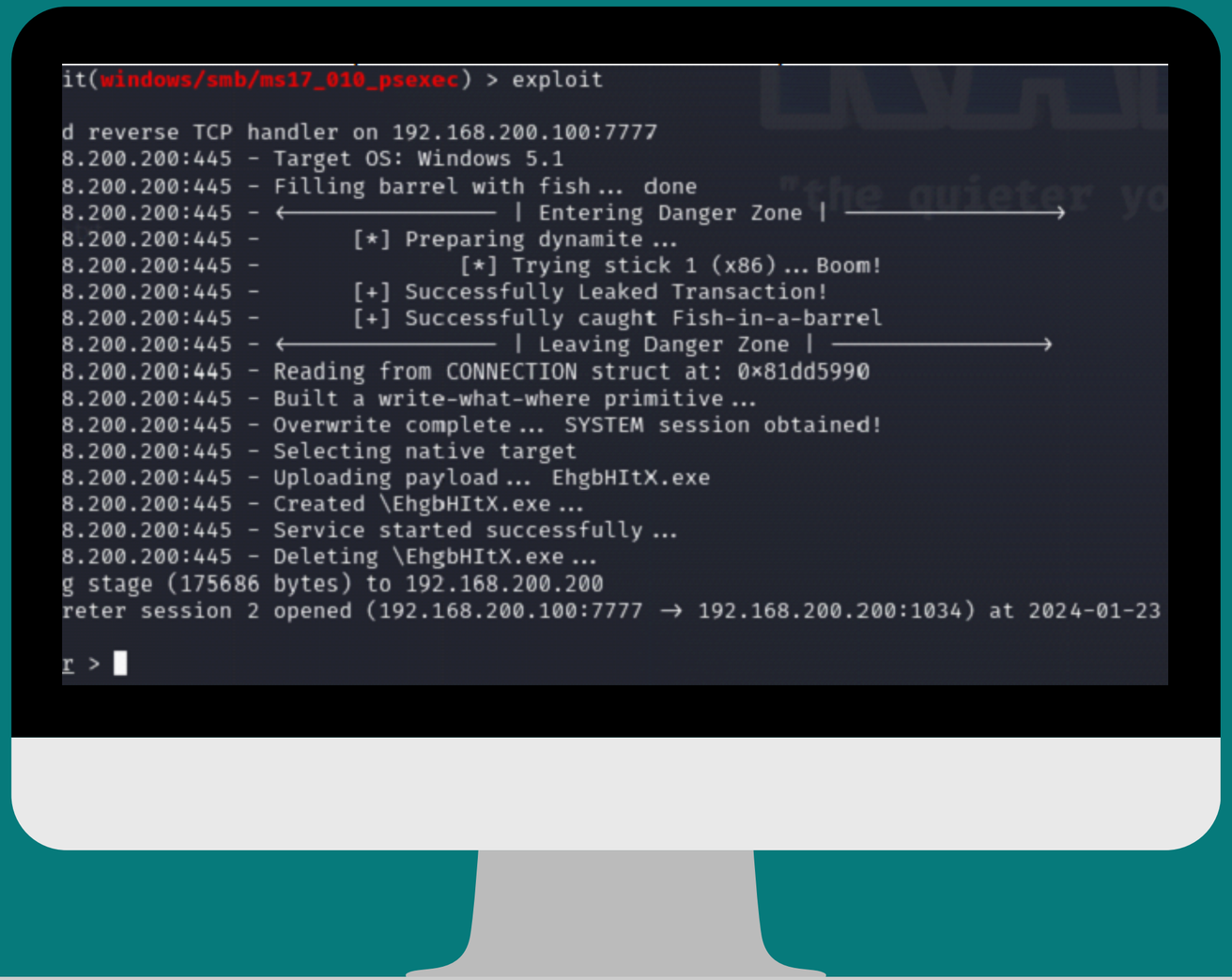
NELL'ESERCIZIO DEL GIORNO 4 SI RICHIEDE DI:

- EFFETTUARE UN VULNERABILITY SCANNING CON NESSUN DELLA MACCHINA WINDOWS XP;
- SFRUTTARE CON METASPLOIT LA VULNERABILITÀ SMB CODE EXECUTION.

ABBIAMO GIÀ CONFIGURATO IL LABORATORIO COME ESEGUITO IN PRECEDENZA.



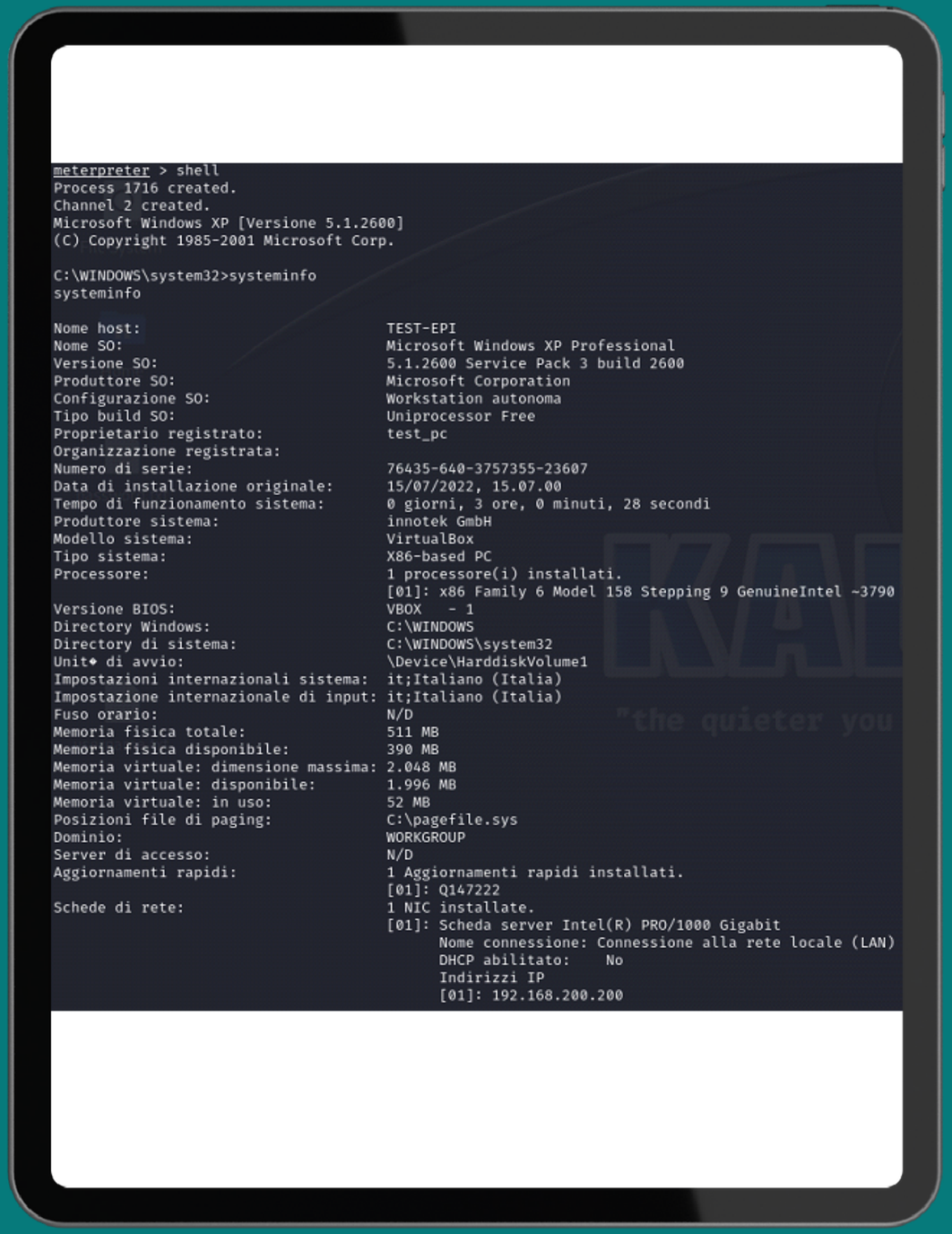
TROVIAMO LA VULNERABILITÀ INDICATA NELLA TRACCIA ATTRAVERSO LA SCANSIONE DI NESSUS.



VERIFICHIAMO SE È POSSIBILE SFRUTTARE QUESTA VULNERABILITÀ PER GUADAGNARE I PRIVILEGI ELEVATI SUL TARGET CON METASPLOIT.
PRENDIAMO IL MODULO CHE DESCRIVE ESATTAMENTE LA VULNERABILITÀ IDENTIFICATA IN PRECEDENZA, CONFIGURIAMO L'INDIRIZZO IP DEL TARGET, L'INDIRIZZO IP DELLA MACCHINA ATTACANTE E LA PORTA IN ASCOLTO SULLA NOSTRA MACCHINA E AVVIAMO L'ATTACCO.

RECUPERO INFORMAZIONI

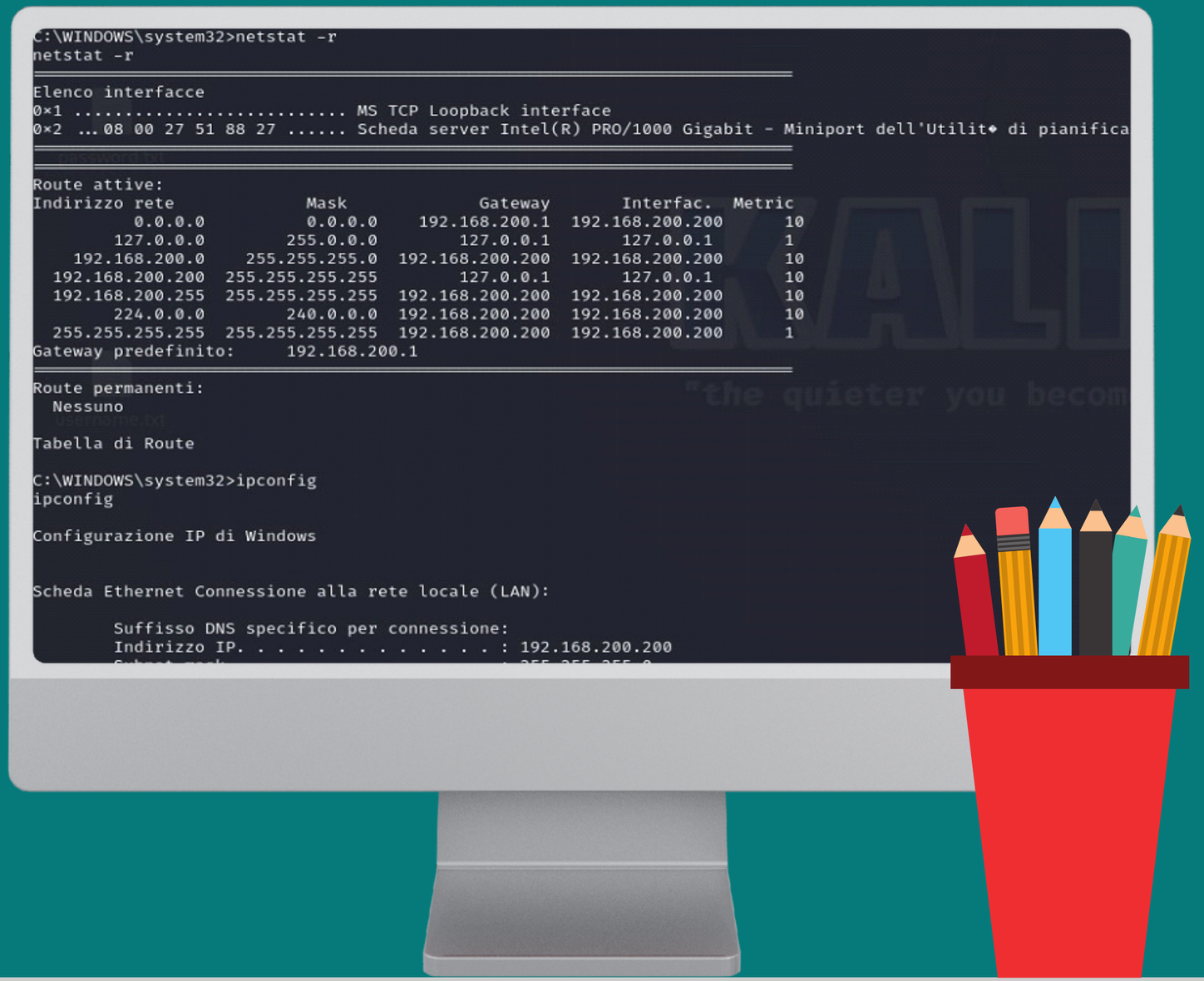
IL TARGET È UNA MACCHINA FISICA O VIRTUALE?



PER OTTENERE QUESTA INFORMAZIONE DOBBIAMO APRIRE LA SHELL DI WINDOWS E INSERIRE IL COMANDO SYSTEMINFO.

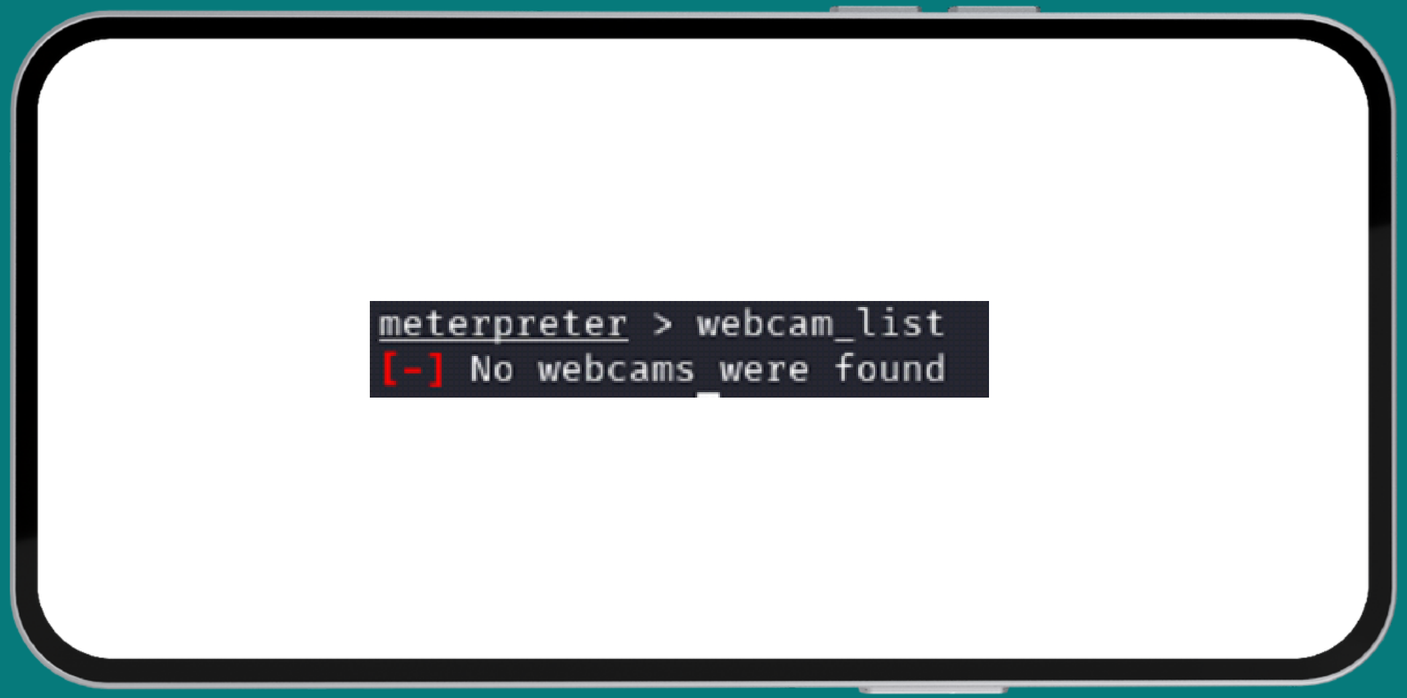
QUALI SONO LE IMPOSTAZIONI DI RETE DELLA MACCHINA?

RECUPERIAMO QUESTA INFORMAZIONE CON IL COMANDO IFCONFIG.



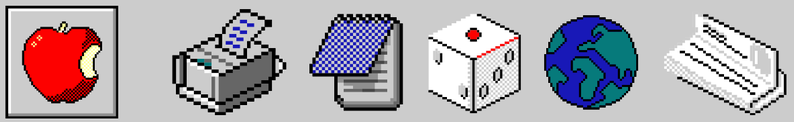
LA MACCHINA HA DISPOSIZIONE UNA WEBCAM?

VERIFICHIAMO CON IL COMANDO WEBCAM_LIST SE CI SONO WEBCAM CONNESSE.

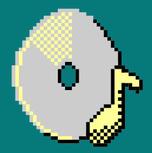


CONCLUSIONI

DATE LE NUMEROSE VULNERABILITÀ PRESENTI E L'INTERRUZIONE AL SUPPORTO DA PARTE DI MICROSOFT, CONSIGLIAMO DI DEPRECARE LA MACCHINA WINDOWS XP E DI SERVIRSI DI UNA AGGIORNATA CON L'ULTIMO WINDOWS DISPONIBILE. NEL CASO NON FOSSE POSSIBILE, ANCHE SE DA NOI NON È PER NULLA CONSIGLIATO, SI PUÒ PROCEDERE DISABILITANDO LA FUNZIONA DI CONDIVISIONE FILE E STAMPANTI

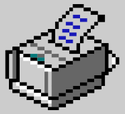


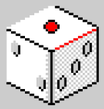



GRAZIE







11:12OPM