esercizi su vulnerabilità del software e delle reti

© 2006-2013 maurizio pizzonia ï sicurezza dei sistemi informatici e delle reti

input fidato e non

Å per quali dei seguenti software una vulnerabilità rappresenta una minaccia? in quali condizioni?

- ï apache: server web
- ï il kernel linux
- ï exim: server smtp
- ï passwd: comando per cambiare la password
- ï login: comando che chiede la password e apre una shell per un certo utente
- ï crontab: comando per schedulare operazioni periodiche da eseguire anche se lôutente non è loggato
- ï ps: comando per vedere i processi attivi
- ï ls: comando per vedere la directory corrente

© 2006-2013 maurizio pizzonia ï sicurezza dei sistemi informatici e delle reti

questo cgi script è vulnerabile?

```
#!/bin/sh
# mostra via web lo spazio libero
# nelle partizioni
echo -e "Content-type: text/html\n\n"
df
```

© 2006-2013 maurizio pizzonia ï sicurezza dei sistemi informatici e delle reti

questo cgi script è vulnerabile?

```
#!/bin/sh
# mostra un traceroute verso
# un ip passato come parametro
echo -e "Content-type: text/html\n\n"
traceroute $QUERY_STRING
```

- in $QUERY_STRING il web server passa tutto ci¸ che, nell'url, ¯ dopo ñ?ò
  - ï es. http://localhost/cgi-bin/tr?193.204.161.1

© 2006-2013 maurizio pizzonia ï sicurezza dei sistemi informatici e delle reti

buffer overflow: il seguente programma è vulnerabile?

```
int main()
   { f(); }
void f()
   {
   char b[30];
   getwd(b) ; /* get working directory */
   printf(ñ%sò, b);
   }
```

© 2006-2013 maurizio pizzonia ï sicurezza dei sistemi informatici e delle reti

buffer overflow: il seguente programma è vulnerabile?

```
int main()
   {
   char b[30];
   getwd(b) ; /* get working directory */
   printf(ñ%sò, b);
   }
```

© 2006-2013 maurizio pizzonia ï sicurezza dei sistemi informatici e delle reti

buffer overflow: il seguente programma è vulnerabile?

```
int main()
   {
   char *b;
   char b2[100];
   b = getenv ("PATH"); /* take the value of
   $PATH */
   é  .
   é  .
}
```

© 2006-2013 maurizio pizzonia ï sicurezza dei sistemi informatici e delle reti

buffer overflow: il seguente programma è vulnerabile?

```
int main()
   {
   char *b;
   char b2[100];
   b = getenv ("PATH"); /* take the value of
   $PATH */
   strcpy(b2, b) ; /* copy b in b2 */
   é  .
}
```

© 2006-2013 maurizio pizzonia ï sicurezza dei sistemi informatici e delle reti

vulnerabile?

- Å questo programma è vulnerabile?
- Å perché?

```
readRecipe (int fd)
{
  char str[200];
  while (readLine (fd, str))
    printf ("%s\n", str);
}
```

```
readline (int fd, char* str)
{
  int n;
  do
    {
      n = read (fd,str, 1);
    }
  while (n > 0 && *str++ != NULL);
  return (n > 0);
}
```

© 2006-2013 maurizio pizzonia ï sicurezza dei sistemi informatici e delle reti

buffer overflow
stack cresce verso lôalto

- come si comportano le architetture con stack che cresce verso lôalto rispetto al buffer overflow?
  - sono più o meno esposte al rischio?

```
int main()
  {
  char b[30];
  scanf (ñ%sò, b);
  }
```

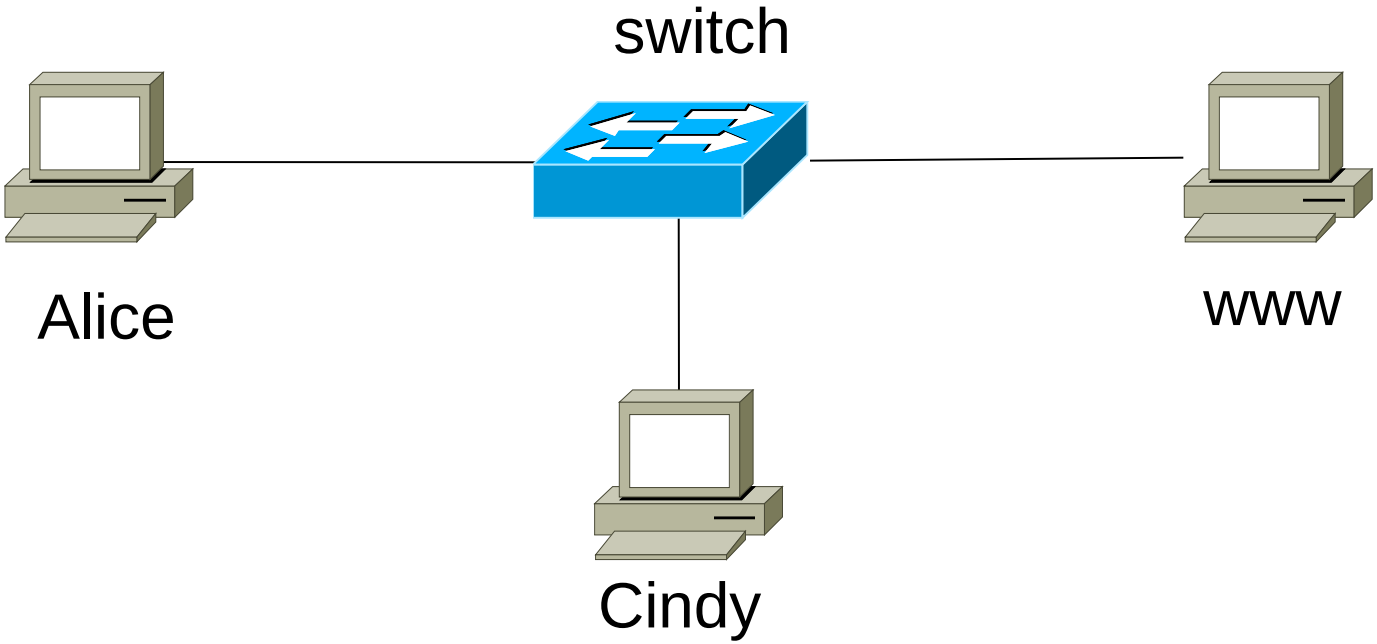
© 2006-2013 maurizio pizzonia ï sicurezza dei sistemi informatici e delle reti

buffer overflow: stack cresce verso lôalto

- Å rivedi tutti i precedenti programmi nel caso di stack che cresce verso lôalto

© 2006-2013 maurizio pizzonia ï sicurezza dei sistemi informatici e delle reti

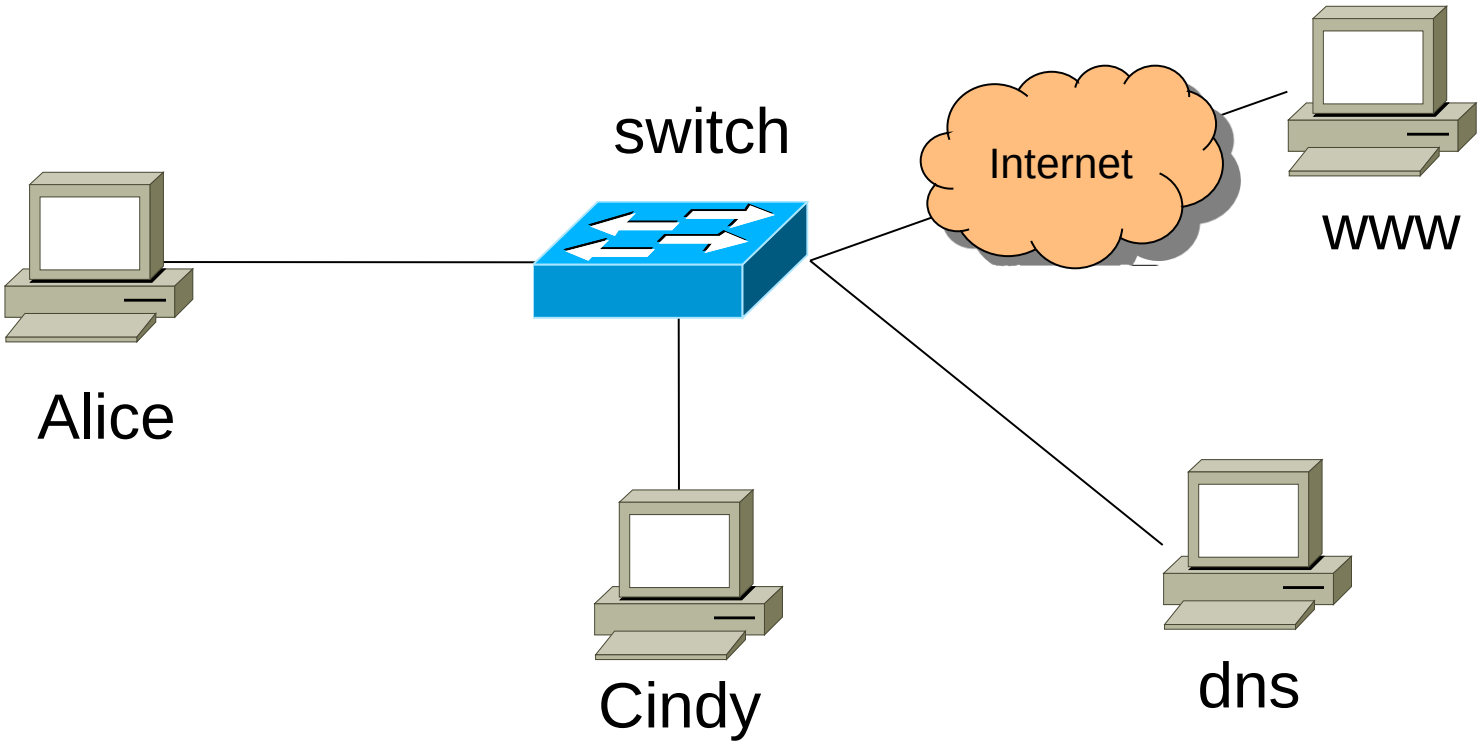
vulnerabilità reti



- Alice dialoga con www, http su tcp
- Come fa cindy a sniffare il traffico?
- come fa Alice o lôamministratore ad accorgersi dellôintruso?

© 2006-2013 maurizio pizzonia ï sicurezza dei sistemi informatici e delle reti

vulnerabilità reti



- Alice accede a www (http su tcp), risolvendo il nome tramite il server dns (non autenticato)
- Come fa cindy a far si che Alice acceda ad un web server sulla sua macchina anziché a www?
- come fa Alice o l'amministratore ad accorgersi dell'intruso?

© 2006-2013 maurizio pizzonia ï sicurezza dei sistemi informatici e delle reti