|  |  |
| --- | --- |
| **Digital Forensics**  Diploma in CSF/IT  Year 2/3 (2022/23) Semester 4/6 | Week 3 |
| Tutorial 3 |
| **Case Study: Investigating Lateral Movement** | |

**OBJECTIVES**

After completing this topic, you should be able to

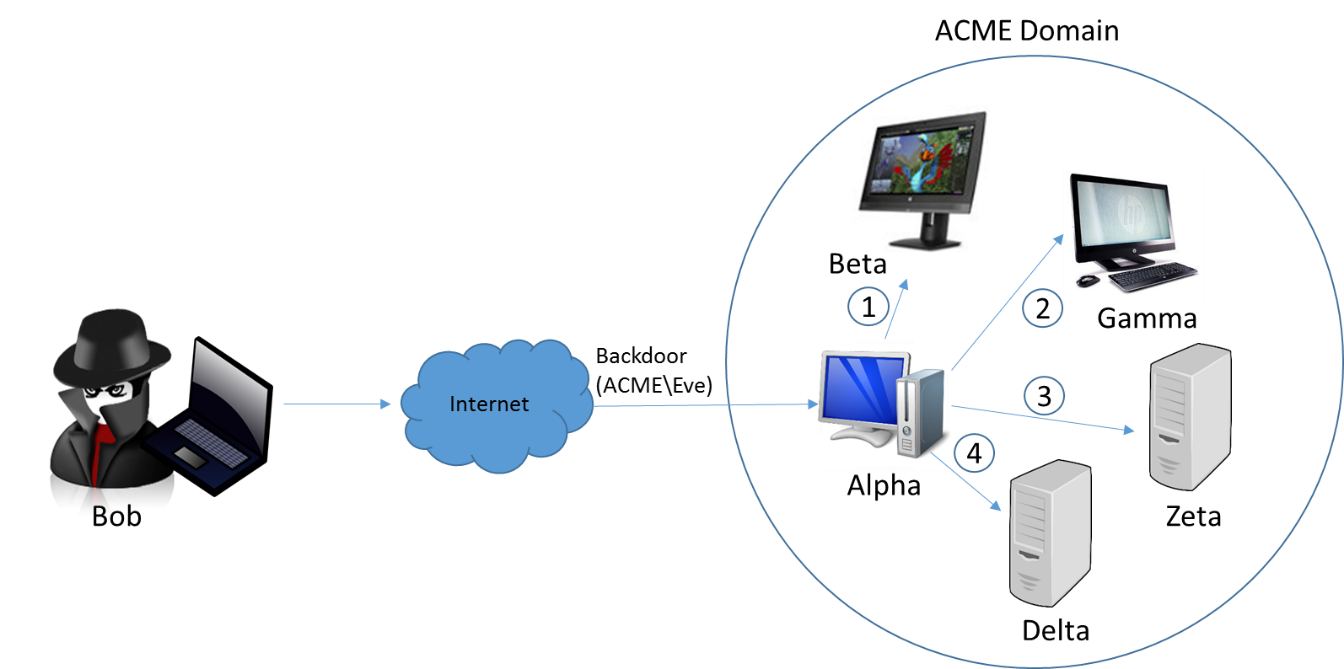
1. Explain how the logon events are created
2. Identify the location where these events can be found

**Background:**

In a compromised Windows environment, attackers typically leverage stolen, valid credentials (either local or domain) to move from system to system – a process known as “lateral movement”.

Many environments use common local administrator passwords for all systems, or subsets of their environment. If an attacker compromise a single system and obtain such a credential, they can move freely from host to host. Worst yet, if the attacker gains access to a domain administrator account, they may be able to access any system within the domain at will.

**Case Description:**



* The attacker, Bob, has interactive access to a Windows 7 workstation, Alpha, through persistent backdoor.
* Alpha is joined to a corporate domain, ACME.
* The backdoor runs under the context of the domain user who owns Alpha, ACME\Eve.
* Through password dumping and other intrusion activities, the attacker has obtained credentials for two accounts:
  + A local administrator, localAdmin, that is configured with an identical password on each workstation in the ACME domain
  + A domain administrator, ACME\domainAdmin, who has full access to all workstations and servers in the environment

Bob uses the backdoor to invoke a command shell under the context of ACME\Eve. He uses various commands, in combination with the credentials for accounts localAdmin and ACME\domainAdmin, to access four systems, each in a different manner:

1. He mounts the C$ share for workstation Beta, from source system Alpha, to transfer malware and tools, using the following command:

net use [\\beta\c$](file:///\\beta\c$) /u:localAdmin “badPassword”

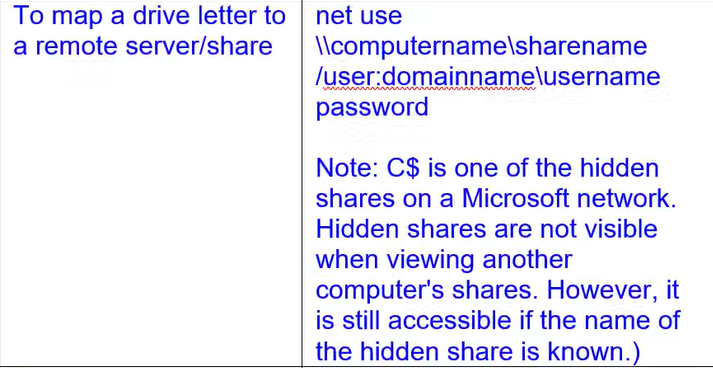
1. He uses the SysInternals PSExec utility to remotely execute a command on workstation Gamma, once again from source system Alpha, using the following command:

psexec.exe [\\gamma](file:///\\gamma) –u ACME\domainAdmin –p worsePassword “C:\path\to\malware.exe”

1. He establishes a remote desktop connection to server Zeta, once again from source system Alpha, using the Windows built-in RDP client (username ACME\domainAdmin, password worsePassword).
2. He browses to an IIS intranet web server, Delta that requires NTLM authentication. Bob uses ACME\domainAdmin credentials.

**Activities:**

Q1: Research online to find out the purpose and syntax of the following commands:



|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Commands** | **Purpose** | **Syntax** |
| 1 | net use | Connects a computer to or disconnects a computer from a shared resource, or displays information about computer connections. The command also controls persistent net connections. Used without parameters, **net use** retrieves a list of network connections. | net use [{<DeviceName> | \*}] [\\<ComputerName>\<ShareName>[\<volume>]] [{<Password> | \*}]] [/user:[<DomainName>\]<UserName] >[/user:[<DottedDomainName>\]<UserName>] [/user: [<UserName@DottedDomainName>] [/savecred] [/smartcard] [{/delete | /persistent:{yes | no}}]  net use [<DeviceName> [/home[{<Password> | \*}] [/delete:{yes | no}]]  net use [/persistent:{yes | no}] |
| 2 | psexec | PsExec is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. | psexec [\\computer[,computer2[,...] | @file]][-u user [-p psswd][-n s][-r servicename][-h][-l][-s|-e][-x][-i [session]][-c executable [-f|-v]][-w directory][-d][-<priority>][-a n,n,...] cmd [arguments] |
|  |  |  |  |

Graphical user interface, text, application

Description automatically generated

Q2: Each of the four actions carried out by attacker Bob above will result in a logon event. Complete the following table to show the Logon Type (refer to Lecture 3, slide 47) and the location where the events are logged.

|  |  |  |  |
| --- | --- | --- | --- |
| **Action** | **Logon Type** | **Location** | **Remarks** |
| 1 | 3 (Network) | Beta | A local account was used |
| 2 | 3 (Network) | Gamme and ACME domain controller  Alpha | A domain account was used  Due to the use of Psexec under a different set of domain credentials than the attacker’s current sesision (ACME\Eve) |
| 3 | 10 (Remoter Interactive) | Zeta and ACME domain controller | A domain account was used |
| 4 | 3 (Network) | Delta and ACME domain controller | A domain account was used |

- End -